NAIC-ID(RS)T-0398-96

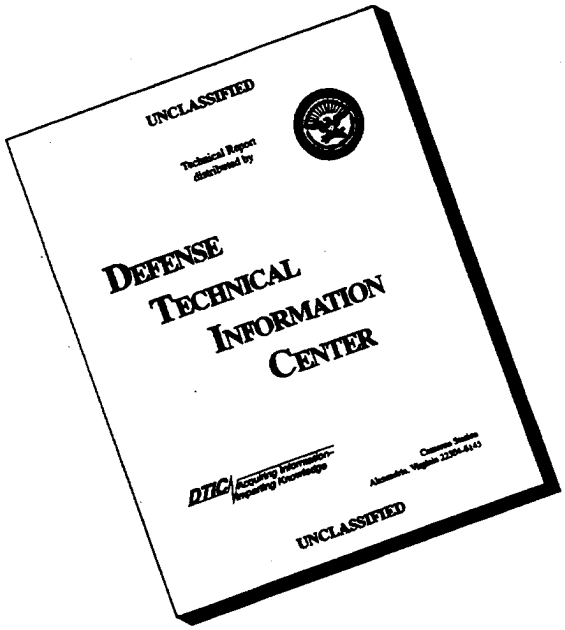
NATIONAL AIR INTELLIGENCE CENTER

SELECTED ARTICLES

19960903 010

Approved for public release: distribution unlimited

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

HUMAN TRANSLATION

NAIC-ID(RS)T-0398-96 24 July 1996

MICROFICHE NR:

SELECTED ARTICLES

English pages: 92

Source: Proceedings of Symposium on Trend and Aspect of Electronic Warfare in 21st Century, 1994, (Cama, Vol. 3, Nr. 1, 1996; pp. I 1-27; 164-179..

Country of origin: China
Translated by: Leo Kanner Associates
F33657-88-D-2188
Requester: NAIC/TASC/Richard A. Peden, Jr.
Approved for public release: distribution unlimited.

TABLE OF CONTENTS

Graphics Disclaimer ii

OPERATIONAL PHILOSOPHY OF ELECTRONIC WARFARE, by Dai Jinxuan 1

NEWLY DEVELOPED CONNOTATIONS OF ELECTRONIC WARFARE UNDER CONDITIONS OF HIGH TECH WARFARE, by Ju Lianyuan 29

THE DEVELOPMENT OF ELECTRONIC WARFARE THEORY AND OPERATIONAL USE OF ELECTRONIC WARFARE IN HIGH TECH WARS, by Quan Shouwen 41

ELECTRO-OPTICAL COUNTERMEASURE TECHNOLOGY FOR GUIDANCE STATIONS (OR PROTECTED TARGETS), by Ji Shiao 63

2-18GHz BIPOLARIZED HORN ANTENNAS USED IN ELECTRONIC WARFARE, by Teng Xiuwen 84

GRAPHICS DISCLAIMER

All figures, graphics, tables, equations, etc. merged into this translation were extracted from the best quality copy available.

NAIC-ID(RS)T0398-96

OPERATIONAL PHILOSOPHY OF ELECTRONIC WARFARE

BY: Dai Jinxuan

In the modern world, the problems of war and peace have become a topic of much concern in the determination of defense strategy of all nations, especially since the collapse of the former Soviet Union with basic changes occurring in the global situation. The situation where the military alliances of the United States and the Soviet Union stood in opposition to each other no longer exists, and the world is moving in a multipolar direction. Political, economic, ethnic and territorial disputes in a number of countries and regions have broken out after having been concealed for a long period of time and have worsened. Major territorial conflicts will grow into new "hot spots" of military conflict. It can be predicted that in the future there will not be a high probability of a major world war, but that the probability is that primary characteristics of wars in the 21st century will be regional conflicts over a limited amount of area, with the selection of limited targets, using high tech methods in order to attain limited objectives. The primary characteristic of this type of regional war "unpredictability". They will break out suddenly without warning. The Gulf War is a clear example of the characteristics of this type of regional war. Therefore, in order to adapt to these tremendous strategic changes all nations are actively making adjustments to their military strategies and defense policies, doing new research into military theory and operational philosophy so they can move in the direction corresponding to high tech regional wars. This paper primarily addresses the special uses and position of electronic warfare in modern high tech regional wars, the types of electronic warfare and the constant expansion of their operational areas as well as new developments in the theory of electronic warfare, presenting a simple analysis of the developmental process of the operational philosophy of electronic warfare.

I. Electronic warfare is an obvious characteristic and the mainstream of high tech regional wars

The first major change in the philosophy of electronic warfare is seen through the promotion of electronic warfare to one of the basic forms of high tech regional warfare. Headquarters at every level must consider electronic warfare as a major component part of warfare, and include it in the operational planning of tactical commanders.

A number of recent regional wars and especially the Gulf War indicate that military electronics is the heart and mainstay of achieving high technology in military actions. With the rapid development of electronics high technology and with the constant expansion of its application in military fields, and with gaining control of the electromagnetic spectrum (airwaves) as the primary objective of electronic warfare, it is necessary that electronic warfare be one of the basic forms and a primary component part of regional wars. For example, during the Vietnam War in the sixties when the Vietnamese forces first used SA-2 surface-to-air missiles to deal with the American air supremacy, at first they averaged shooting down one American aircraft with every eight to eleven SA-2 missiles fired, resulting in an American plane loss rate of 14 percent. However, the Americans quickly became aware that electronic warfare was an effective method against attacks by these missiles, and they developed an emergency plan, developing and equipping their forces with electronic warfare equipment, gradually forming an air superiority operational electronic warfare system of primarily airborne self defense electronic warfare equipment in conjunction with EB-66 electronic warfare aircraft and F-4 and F-105 "Weasel" anti-radar aircraft, effectively suppressing he Vietnamese forces' tight radar network and air defense firepower network. By the end of 1968 the Vietnamese forces only averaged

one American plane shot down for every 70 to 80 SA-2 missiles, and the loss rate of the American planes quickly dropped from 14 percent to 1.4 percent. During the "Rear Guard" action of 1972, eight or nine B-52 bombers were sent out every night, with two to three EB-66 electronic warfare aircraft and from four to eight F-4 and F-105 anti-radar aircraft, with a ratio of 1.2-to-one to two-to-one electronic warfare aircraft to bombers. At the same time, all sorts o tactical aircraft were all equipped with self defense electronic warfare equipment. In this action, the Vietnamese forces launched more than 1,000 SA-2 missiles and only shot down 15 B-52 bombers. The Americans estimated that if they had not used effective electronic warfare, it is possible that they would have lost 75 B-52 bombers. The Americans ability to easily break through defenses and bomb North Vietnam was due to electronic warfare. Therefore, electronic warfare grew during the Vietnam War into a major means of countering missile attack.

In June of 1982 during the war in Syria's Becca Valley Israel used electronic warfare as a major element of its combat forces, forming an AWAC systems with E-2C and "Scout" and "Mengquan" (phonetic) drone aircraft. Boeing 707 electronic warfare aircraft, F-4G anti-radar aircraft and advanced airborne self defense electronic warfare systems composed an aerial electronic warfare system primarily directed against Syrian C^3I and SA-6 missile positions, conducting fierce electronic interference and anti-radiation missile attacks. In the first six minutes 19 Syrian SA-6 missile positions were completely destroyed, 79 Syrian aircraft were shot down without the loss of a single Israeli combat aircraft, thus establishing a glorious example of using electronic warfare to suppress air-defense.

In the American air raids of Libya in 1986 the electronic warfare was even more intense. The Americans launched 19 of the

most advanced DF-111A and EA-6B electronic warfare aircraft and six F-18 fighters equipped with "Shrike" anti-radiation missiles. The ratio of electronic warfare aircraft to strike aircraft was between one-to-four and one-to-six. After the american aircraft took off, they used electronic warfare aircraft to carry out intense electronic jamming to suppress Libyan ground detection, warning and guidance radars and command and communications facilities. They used "Hamu" (phonetic) anti-radiation missiles and "Harpoon" anti-radar missiles to directly destroy these facilities, blinding Libyan radar and cutting off their communications. The Libyans launched seven SA-2 and SA-5 surface-to-air missiles, but with the intense jamming by the American aircraft, not a single one hit a target, allowing the American aircraft to return victoriously after completing their raids on their targets, once more setting a successful example of using electronic warfare to first "blind" the enemy, and then using "surgical strikes".

If we say that electronic warfare first began to be used as operational methods in the regional wars in the eighties, then by the Gulf War in 1991 electronic warfare had already become elevated to a primary component of regional wars. In this war, the Multinational Forces deployed a unified land, sea, air and space electronic intelligence reconnaissance network with more than 100 EF-111A, EA-6B, EC-130H and F-4G special electronic warfare aircraft, and more than 1000 airborne self defense electronic warfare systems and seven aircraft carrier group ship-borne electronic warfare facilities to form an electronic warfare network that omnidirectional, all altitude, total spectrum and multiple method multiple channel and three dimensional. This ensured that the Multinational Forces could conduct continual reconnaissance and surveillance of Iraqi territory and using its strong electronic warfare attack forces, conducted a concentrated, dense electronic

jamming to suppress and anti-radiation missile to attack the Iraqi air defense system, thus injecting a strong a positive entropy flow into the Iraqi air defense system, causing drastic disorder, and thus resulting in Iraqi radars in being blinded, weapons to be useless, communications to be cut off, command to be disrupted, and the entire C^3I system to be blind, deaf and mute. The air defense system was completely paralyzed and unable to organize an effective counter attack. The commander of the American Naval reserve forces, Admiral "Xier" (phonetic) pointed out that "during the first hours of combat we struck a ferocious blow the to Iraqi C^3I system, and they were never able to recover from it." General "Caluoer" (phonetic) of the American Defense Intelligence Center stated that "faced with the soft weapons of electronic warfare, the Iraqi air forces clearly had no combat capability. We have used jamming aircraft and decoy's to severely paralyze their systems. They cannot see us coming, and their anti-aircraft guns keep shooting blindly". An American electronic warfare officer stated that "when there was an F-4G anti-radiation missile attack aircraft in position, not a single Multinational force aircraft was shot down by a radar guided weapon." It is claimed that the United States launched a total of 1000 "Hamu" missiles, destroying about 250 Iraqi air defense radars. Clearly in this war the many different types of electronic warfare weapons used by the Multinational Forces, their high level of technology, their large scale, the degree to which they were coordinated are all unprecedented in modern warfare. The number of electronic warfare aircraft was more than ten percent of the total number of aircraft, and in the air raid operations, about 20 percent of the total number of aircraft used conducted electronic warfare missions. It was because the Multinational Forces made composite use of the different types of advanced electronic warfare equipment and operational methods along with clever tactics, using strong electronic warfare attack forces to suppress the fairly strong

Iraqi airforces which lacked electronic warfare capability, effectively ensuring that their operational actions were carried out in an orderly manner, that the American aircraft losses were reduced to a historically low level of 0.04 percent of the 110,00 sorties launched in 38 days. Therefore, the victory of the Multinational Forces in the Gulf War was actually a victory of electronic warfare.

It is easily seen in these regional wars and especially in the Gulf War that due to the fusing of military electronics high technology and modern military methods and the tremendous increase of battlefield electromagnetic factors have led to electronic warfare with its goal of seizing "control of the electromagnetic spectrum" having become a basic form and major component of modern high tech regional wars. The outstanding characteristics of these types of wars are: Combatants on both sides will possess C^3I systems with high technology capabilities, comprehensive electronic warfare systems and precision guided weapons are used to conduct fierce system against system confrontation by all three branches of the service. Each military action taken on the battlefield will first be preceded by suppression of the other side's various types of electronic equipment and precision guided weapons and to ensure one's own similar equipment is used effectively. Victory or defeat will primarily be determined by the engagement of the comprehensive combat forces of both sides's composed of electronic equipment and high technology weapons which rely on electronics technology. In the high technology battlefield of the 21st Century there will be no simple formula for victory, but only a few key elements for success, including the major key element of electronic warfare providing the joint forces with soft and hard kill weapons support capability. Therefore, in future regional wars "electronic warfare will surpass the roles of traditional combat support and will have a direct effect on the progress of the war. A former commander of

NATO pointed out that "in future wars the only systems which are complete systems will be those which give full consideration to electronic warfare and to modern weapons systems. No headquarters at any level will be able to eliminate the comprehensive use of electronic warfare measures. Electronic warfare is a combat means which has a great deal of combat strength. It is also recognized to be a weapon which can be used in wars of all scales. Any headquarters which lacks careful consideration of electronic warfare cannot be considered to be a headquarters." Admiral T. D. Tayler of Naval Operations pointed out that "considering how lethal modern weapons are, survivability will be the basis of future wars and to achieve an appropriate degree of survivability, the effective use of electronic warfare is extremely important." Following the Gulf War a number of foreign military commentators pointed out that "this war was a victory of silicon over iron", "was a victory of electronic warfare", "the electronic warfare which has been propagandized for the past ten years was proven in the Gulf War, and it played an extremely decisive role in the victory in the overall campaign" It can be predicted that as high technology becomes widely used in all fields in the military, it will break through the technological framework in future regional wars, bringing about a competition for superiority in high technology characterized by the information age. This competition will begin with a struggle for superiority in precision guided electronic weapons, and at the heart of these electronic weapons is the electronic guidance system, so after precision guided weapons have unquestionably replaced modern weapons and become the main comb at force, the focus of the competition will shift to the electronic warfare forces centered around the soft and hard kill electronic warfare weapons. During attack, effective electronic warfare can result in disrupting the enemy's C^3I systems, paralyzing air defense systems, thus quickly altering the balance of forces between the two sides, turning this balance of forces to

one favorable to one's own attacking forces so they can effectively break through enemy defenses and accelerate the progress of the war and affect the combat situation. During defense, effective electronic warfare can cause the enemy's precision guided weapons to fail, greatly reducing the probability of their hitting their targets and causing damage and delaying the progress of the combat, thus switching one's disadvantages to advantages. Therefore, with such a great reliance of military confrontation on military electronics high technology, electronic warfare has not only become the precursor and guarantor of fire power assaults, but is also used for the direct suppression of C^3I systems, attacks on the enemy's air defense and AWAC systems, thus resulting in the overall collapse of the "force multiplier" of the enemy's combat strength. Therefore, invisible electronic warfare has taken a completely new role on the stage of regional wars, attracting even more attention. In future high tech wars of all forms, the curtain will be raised with electronic warfare, and electronic warfare will permeate the entire process of the war. It will determine the progress of the war and the situations of the war. This is the mainstream and a clear characteristic of future high tech regional wars. Today, if a single country wants to win a modern high tech war, especially a high tech regional war, lack of effective electronic warfare capability is a fatal weakness. Electronic warfare forces will determine how much combat strength a country has. Victory in a modern war will "belong to the side which can effectively control and use the electromagnetic spectrum". This is a major development in the operational philosophy of electronic warfare under conditions of high technology.

II. Electronic warfare methods and operational areas continue to be expanded, increasing the overall combat capabilities of electronic warfare.

Combat experience tells us that the development of weapons and equipment is the basic motivation for changes in operational methods and operational philosophy. The widespread application of military electronic high technology has greatly increased the combat effectiveness of weapons and equipment. When the magnitude of these changes reaches a certain degree, it will necessarily lead to quantitative leaps in the operational methods and operational philosophy, thus resulting in a number of different new operational methods, operational areas and operational philosophies occurring in the next century in electronic warfare. These will include the following:

1. Electronic intelligence warfare is the precursor and the prologue to high tech regional wars

Currently, under high tech conditions, the degree of horizontal and vertical transparency of the battlefield has been greatly increased to the point that in future regional wars all targets which do not have excellent concealment will be detected, and any target detected can be hit, and any target which is hit can be destroyed. Therefore, in such a battlefield environment, an important operational principle of high tech regional wars is to detect targets before the enemy does, to analyze the battlefield situation before the enemy does and to make decisions and take actions before the enemy does. In order to realize this principles, the collection, analysis and rapid dissemination of battlefield military intelligence, command decisions and command coordination, optimum use of combat resources, execution of operational actions and logistic support and even the final victory in combat will all depend to an even greater degree to timely, accurate and reliable electronic intelligence information. The increasing dependence on information in such military action indicates that on the high tech battlefield, actions are determined

on the basis of electronic intelligence, and electronic intelligence will play a role throughout the entire process of the war. It is a huge amorphous combat force. Whoever has the better intelligence collection capability will have the advantage in the war, will have the initiative, and he who has the inferior intelligence collection capability will be in a passive situation and will take a beating. During the Gulf War one key element in the victory of the Multinational Forces was a tightly organized surveillance system including photographic surveillance satellites, electronic surveillance satellites, defense warning satellites, electronic surveillance aircraft and ground electronic surveillance sites which provided a multiple surveillance method, layered arrangement and tiered coverage. It formed an omnidirectional, multiple layer, multiple frequency and multiple method and multiple channel constant electronic/image intelligence surveillance network against Iraq, ensuring the Multinational Forces with large area, constant military intelligence surveillance and monitoring against the military facilities and military actions within Iraqi territory, providing large amounts of detailed intelligence and data for strategic and tactical decision making by the Multinational Forces. It clarified the capabilities, technical parameters and operational characteristics of Iraq's major air defense radar networks and communications networks, allowed the Multinational Forces to have a precise handle on major strategic targets within Iraq and the properties and geographical coordinate of Iraqi military facilities. It created the necessary preconditions for successful electronic interference and assaults during the Multinational Force air raids. Therefore, under conditions of modern electronic warfare, the establishment of a three dimensional electronic intelligence surveillance system which meets the conditions of electronic warfare in order to ensure one's own forces effectively control and make use of the different electronic methods, for detection and surveillance of the

electromagnetic environment around the battlefield and to correctly determine the enemy's military deployment and operational intentions, and the establishment of a strong electronic interference and anti-radiation missile attack system to prevent the enemy from using the different intelligence surveillance systems are keys to victory in modern electronic warfare. An August 22, 1990 article in the French newspaper "paris Daily News" stated that "the Gulf War has begun, and even though at the present time it is a quiet war, the destruction it has caused among military persons is like that of a conventional war."

2. C^3 countermeasures are important measures to win victories in high tech local wars.

The Gulf War was actually a war between two huge opposing weapons systems. The Multinational Forces launched between 2000 and 3000 sorties of about 20 different types of aircraft and 40 different models in its bombing raids. For so many aircraft from so many countries to be able to orderly launch accurate raids on predetermined Iraqi targets, the Multinational Forces relied primarily on a highly automated C^3I system for coordination and guidance so these bombing raids could have the best overall combat effectiveness. The C^3I system was able to provide commanders with accurate, timely and reliable battlefield information, provide processing, display and evaluation of threats, so they could determine the best decisions, carry out combat preparations, send operational orders to subordinate units and monitor, control and coordinate the operations. Therefore the C^3I systems could take the four major military steps of detection, evaluation, decision making and action and connect them into a loop, becoming the battlefield "nerve center" and "eyes and ears". The commanders could use the C^3I systems to introduce the appropriate force at the proper time and place to achieve large operational results at a

fairly small cost. In future regional wars, C^3I systems will be able to act as a "force multiplier" of the overall operational capabilities. However, the C^3I system is supported by large amounts of military electronic equipment, so by using such electronic warfare measures as electronic jamming and deception, destruction by anti-radiation weapons, blinding by microwave weapons and throttling the enemy "nerve centers" by using computer viruses, thus resulting in loss of control of groups of high tech weapons, interruption of information, disruption of command, loss of coordinated combat capability, greatly weakening the enemy's combat strength or even completely losing his combat capability. During the Gulf War, in the multinational Forces' first strategic bombing raid, electronic aircraft were used first in coordination with "Tomahawk" missiles and other C^3 countermeasures in a fierce "electronic bombardment" and assault on Iraq's key C^3I links such as the air defense radar network, and command and communications network, result in Iraq's C^3I system becoming "blind", "deaf" and "mute", thus resulting in the total collapse of the entire air defense systems so they were unable to organize a strong counterattack. Therefore, the Gulf War shows that C^3 countermeasures aimed primarily at C^3I will be a major countermeasure in future regional wars, and electronic warfare is a core component and operational method of C^3 countermeasures.

3. With the use of large numbers of precision guided weapons on the battlefield, guidance and counter guidance will continue to be a major operational area of electronic warfare

Precision guidance is the direction in which high tech conventional weapons are being developed. Millimeter wave and optoelectronic technology has been used in large amounts in these weapons, and these technologies have been combined with information processing and display technology resulting in the rapid

development of "fire and forget" precision guided weapons. Compared to unguided missiles, precision guided weapons have a one to two order of magnitude increase in range, speed and hit accuracy, with a hit rate of almost 100 percent. For example, during the Gulf War the United States "multiple tube rocket launcher systems" launched 12 rockets in a single volley could launch 7728 infrared guided "Sijite" (phonetic) bomblets which could attack most of the tanks in a tank company. A single AH-64 helicopter gunship can carry 16 "Hellfire" semi-active laser guided missiles which can attack two tanks at once, increasing anti-tank capabilities by 20 fold. With the development of microwave and infrared imaging guided container bombs and submissile technology, one missile (such as the U.S. Army tactical missile system) can contain hundreds of cluster bombs with terminal guidance, each one of which can attack a tank, with an order of magnitude increase in the number of targets which can be attacked, and with the power comparable to a small nuclear device. During the Gulf War the Multinational Forces concentrated all the newest precision guided weapons including guided missiles, bombs and guns in attacks on Iraqi major strategic targets and military installation with a hit rate of over 90 percent (non-guided weapons had a hit rate of only 25 percent). Most of the Iraqi targets were destroyed by precision guided weapons. Therefore, precision guided weapons are basically able to achieve destruction of one or multiple targets each time they are fired. They will be basically able to render invalid the basic principle that "numbers have the advantage" for all conventional weapons, where the number and power of the weapons exceed the number of targets and their ability to withstand a hit, and will have a major influence on future military confrontations. However, electronics guidance systems are the heart and soul of precision guided weapons, and a number of recent regional wars indicate that the use of electronic jamming can cause more than 80 percent of precision guided weapons to deviate from their targets.

Therefore, the struggle between guidance and anti-guidance countermeasures continues to be a major confrontational form for future regional wars, and electronic warfare is still the most effective method for countering precision guided missiles.

4. Stealth and anti-stealth countermeasures

In the past ten years, there have been breakthrough advances in stealth weapons which primarily reduce the "detectible" signal characteristics of an attacking target. The United States F-117A stealth fighter bomber was given the initial assault mission in the Gulf War, and they reached Baghdad undetected where they destroyed with precision bombing more than 80 strategic Iraqi targets, achieving the first successes in the war. The F-22 stealth fighter and the B-2 stealth bomber are also being test flown, and at the present time an electronic intelligence recon aircraft called the "AURORA" is being developed. The former Soviet Union 1-42, also called the MIG-35) stealth fighter has also taken its maiden flight. England, France, and Italy are jointly investing 20 billion Dollars to develop the ACA stealth fighter. It is predicted that by the year 2000 there will be thousands of stealth aircraft in service around the world. Stealth aircraft are able to penetrate enemy strategic and tactical defense networks to conduct a concealed, sudden, precise and ferocious attack on predetermined targets. They are a conventional threat force on the modern battlefield. Their widespread use will necessarily change the nature and structure of national air defense systems and they will constitute a serious threat to defense systems. Therefore, the appearance of stealth aircraft will open the curtain on the stealth and counter stealth struggle. Counter stealth technology is being researched in all frequencies, times and space. Passive detection technology and microwave beam weapons are effective means of countering stealth weapons. The stealth counter stealth struggle

is becoming a new concept for future regional wars.

5. The expansion of new military capabilities of electronic warfare will be the trend of future regional wars

The formation and utilization of the concept of electronic warfare will necessarily prompt continuous development of new generation "new electronic weapons", which will form new operational areas for electronic warfare. For example:

Microwave beam weapons are becoming "new model electronic weapons". These weapons use electromagnetic energy instead of chemical explosive energy to destroy operational platforms and electronic equipment. Because they are three to six orders of magnitude more powerful than traditional radar jammers, they can use low power to jam the electronic equipment on enemy platforms so they are unable to operate normally, or use high power to fry the electronic circuits. They are called "super jammers" or "electronic assassins". For example, the United States Houghes Corporation has already developed a type of high power microwave wavebeam weapon (plasma assist slow wave oscillator) which operates on the C band. Band width is 100μs, and band pulse is between three and five megaHertz. Energy conversion efficiency is as much as 15 to 25 percent. it can fry the electronic equipment in a weapons system. The TOMAHAWK" cruise missile the United States used in the Gulf War has used a warhead which combines a microwave wave beam and ordinary explosives. It converts the energy of ordinary explosives to an electromagnetic pulse (power of 10^9 Watts and duration of 10^{-12} seconds) which destroys the electronic equipment in weapons systems. This type of weapon can only be used one time, so the United States is developing a high power microwave wave beam weapon which can be used repeatedly. Clearly, the successful development of this type of focused energy weapon will

signal the birth of a new generation of electronic weapons, so a new military force in electronic warfare will have to be how to counter focussed (or directed) energy weapons. The United States has already formally listed the capability of destroying directed energy weapons as a new concept in electronic warfare.

Because computers are almost universally used in modern weapons systems and command and control methods, the appearance of computer viruses to destroy information processing and command methods will result in computer virus counter measures becoming a new arena for military confrontation in electronic warfare. Once computer viruses are introduced into the computer networks of C^3I systems, they can paralyze the C^3I network so that they lose their capability of commanding operational units and controlling weapons. The United states Central Intelligence Agency and National Security Agency have already taken the hint from computer viruses which have already appeared, and have quickly invited bids on the development of "military viruses" and "code viruses" in an attempt to affix these into the integrated circuits of exported computers where they could lay dormant for long periods of time, but if war should break out they could be activated remotely, paralyzing enemy military information systems. Therefore, computer virus countermeasures have moved from the conceptual stage to the demonstration stage and even practical stage (it is claimed that during the Gulf War the United States military introduced computer viruses into Iraqi "Exocet" missile computers in Jordan), thus creating a new more effective operational means for electronic warfare.

In summary, as such electronic weapons as C^3I systems, precision guided weapons, stealth weapons, directed energy weapons and computer virus countermeasures are about to be widely used in all areas in modern wars, the three dimensionality of modern warfare will be even further increased, and offensive and defensive

actions will all occur along a broad front, in depth, multiple layers, omnidirectional and multiple spectrum wide band with rapid changes. Faced with this three dimensional multi-faceted battlefield environment, the targets of electronic warfare will be expanded from radars and communications countermeasures to dealing with the overall command and control system of the enemy and the control and guidance systems of high tech weapons. It will be on the ground, in the water, air and space. It will be used along a wide front and in depth, Its frequencies will include transmission frequencies, infrared and laser. Its functions will take into consideration comprehensive countermeasures against radars, communications, guidance and IFF as well as high tech weapons control and guidance systems. Therefore, the simple adding together of single pieces of electronic equipment, single functions or multiple types of electronic warfare equipment will not be able to ensure effective and reliable suppression of enemy comprehensive electronic weapons, but it will be necessary to use electronic warfare systems from multiple platforms, of multiple types, multiple frequencies and multiple applications as well as combining electronic warfare methods to form an omnidirectional, multiple layered, multiple frequency spectrum and multiple method operational system which has functional compensation capabilities in order to maximize the overall combat effects of electronic warfare and meet the system countermeasure requirements. Therefore, there have been major strategic changes in the operational philosophy of electronic warfare. The general guiding philosophy is: Focussing on the characteristics of future high tech regional wars and the general direction of development of high technology, use system countermeasures as the primary guiding philosophy of electronic warfare operations with the weak links in enemy command and control systems and weapons control and guidance systems as the primary operational targets. Establish a unified land, sea air and space electronic surveillance systems for three

dimensional surveillance and close monitoring of the theater electromagnetic threat. Conduct timely intelligence support. Strive to develop a three dimensional arrangement of a comprehensive electronic warfare capability including soft and hard kill capabilities. Combine the use of high technology electronic warfare equipment and different types of electronic warfare measures with close coordination to form an independent, integral, comprehensive electronic warfare operational system. Make full use of superiority in electronic warfare. Increase the comprehensive combat capabilities for campaign level electronic warfare and have electronic warfare penetrate throughout the entire process of a campaign, penetrating to all areas of the battlefield and each link of campaigns and battles, striving to paralyze enemy C^3I systems in order to cause the collapse of the enemy's overall combat capability and to reduce as much as possible the hit rate of enemy precision guided weapons. Reduce the effectiveness of precision guided weapons. Resulting in bringing the overall war machine to a halt. Therefore, with the constant expansion of new types of electronic warfare operations and operational fields, strengthening the overall operational capability of electronic warfare is a major indication of the development of current electronic warfare operational philosophy.

III. New developments in electronic warfare theory

As electronic warfare has been elevated to the mainstream of modern high tech regional warfare and the constant expansion of the operational fields of electronic warfare, the traditional concept of low level electronic warfare is no longer able to contain the daily increasing contents of modern electronic warfare, and is even less able to demonstrate the tremendous effects that high technology have had on modern warfare, especially on high tech regional wars. Therefore, the operational philosophy of electronic

warfare is gradually being changed and expanded in order to express how electronic warfare high technology has changed the look of high tech regional wars with characteristics of the information age.

In 1990 the United States Joint Chiefs of Staff announced in a memorandum that it had redefined electronic warfare as "electronic warfare is the use of electromagnetic energy to detect, take advantage of and weaken enemy use of the electromagnetic spectrum, or to use damage or destruction to prevent the enemy from using the electromagnetic spectrum, while at the same time ensuring own military actions using the electromagnetic spectrum." This new definition clearly places weapons systems which use electromagnetic energy such as anti-radiation missiles and anti-radiation drone aircraft within the scope of electronic warfare, thus providing electronic warfare with new military capabilities to damage and destroy enemy systems. This indicates there is already a clearly offensive nature to electronic warfare.

Following the Gulf War, it was held at the highest levels within the United States armed services that the tremendous success of "Desert Shield" and "Desert Storm" in the Gulf War demonstrate that electronic warfare is a vital multiplier of military force in all operational areas. In modernized joint operations, there have been major changes in the overall field of electronic warfare including the definition, operational philosophy, weapons use and operational methods of electronic warfare. The concepts of electronic warfare which have been in use for many years are not longer suited to the realities of modern warfare. Therefore, the United States Joint Chiefs of Staff adopted a series of actions, recently announcing the new definition of electronic warfare and C^3 countermeasures in memorandums MOP6 and MOP30. In MOP6 the new definition of electronic warfare was: Any military action using electromagnetic energy or directed energy to control the

electromagnetic frequency spectrums or to attack the enemy. Electronic warfare includes three major components: Electronic attacks, electronic protection and electronic warfare support.

• Electronic attack: This is a component part of electronic warfare, and it includes the use of electromagnetic energy or directed energy in an attack on personnel, installations or equipment with the purpose of weakening, inhibition or destruction of enemy combat capability.

• Electronic Protection: This is a component part of electronic warfare. It includes electronic warfare conducted to protect personnel, facilities and equipment or the various actions taken to ensure that enemy use of electronic warfare to weaken, inhibit or destroy ones own combat capabilities is not effective.

• Electronic warfare support: This is a component part of electronic warfare, and it includes the various actions undertaken to search for, intercept, recognize and locate intentional or unintentional electromagnetic radiation under the direct control of operational commanders in order to achieve immediate recognition of threats. Therefore, electronic warfare support provides the necessary information for timely decision making. This decision making includes electronic warfare operations, threat avoidance, target instructions and other tactical actions.

The relationship among the component parts of the newly defined electronic warfare are shown in a later illustrations.

After the Gulf War, the United States military believed that the important role of C^3 countermeasures in modern warfare was becoming increasingly prominent, and they placed special emphasis on countering potential enemy command and control capabilities. In

view of the fact that the existing definition of C^3 countermeasures was conceptually too narrow, and that it placed excessive emphasis on countermeasures directed against equipment and did not stress that C^3 countermeasures were a strategic element. This led to a degree of misunderstanding that C^3 countermeasures were merely a type of operational method for countermeasures directed at equipment and which ignored that it was an overall command and control capability operational policy which made use of all operational resources which can be mobilized to destroy the enemy including human factors. Therefore, the United States Joint Chiefs of Staff published the memorandum on policy MOP30, which changed the name of C^3 countermeasures to command and control warfare, abbreviated C^2W, which is defined as: With the support of intelligence, the comprehensive use of electronic warfare, military deception, operational security, psychological warfare and physical destruction to prevent the enemy command and control (C^2) capability from obtaining information, and to influence, weaken or destroy enemy command and control capabilities, and at the same time ensuring that our own command and control capabilities are protected from similar affects. C^2W is used throughout the entire operational areas in combat at all levels. It includes counter C^2 and C^2 protection.

Counter C^2 is defined as by preventing the enemy from obtaining information, influence, weaken and destroy enemy C^2 systems, and prevent the enemy from effective command and control over its subordinate units.

C^2 protection is defined as keeping the enemy from preventing our own C^2 system from obtaining information, and thus influencing, weakening or destroying our own C^2 capability, and ensuring the effective command and control of our own units.

Relationships in the new definition of electronic warfare

1. Electronic warfare. 2. Electronic attack. The use of electromagnetic or directed energy to attack personnel, facilities or equipment in order to weaken, inhibit or destroy enemy combat capabilities. 3. Electronic Protection. Any action taken to protect personnel, facilities and equipment so combat capability is not weakened, inhibited or destroyed by enemy use of electronic warfare. 4. Electronic support. The search for, intercept, recognition and locating of radiating electromagnetic energy sources as directed by operational commanders or directly under their control while electronic warfare operations or other tactical actions (such as threat avoidance, homing and target guidance) are being conducted in order to immediately recognize threatening actions. 5. Anti radiation missiles. 6. Directed energy. 7. Jamming. 8. ECM deception. 9. Operational directional finding. 10. Operational threat warning. 11. Radiation control. 12. ECM protection. 13. ECM tuning. 14. Other ECM methods.

Clearly electronic warfare and command and control warfare as newly defined by the United States Joint Chiefs of Staff enlarges and develops the theories and operational philosophy of electronic warfare. It formally illustrates that electronic warfare has been elevated to a primary component of modern high tech warfare and to a core component part of the elements of combat strength. This is primarily seen in the following:

• Electronic warfare is an offensive military action. The newly defined electronic warfare uses active assaults with electronic attacks (EA) to replace the electronic jamming and electronic deception (ECM) of the old concept of "self defense". This clearly stipulates the use of electronic jamming, electronic deception, anti radiation weapons and directed energy weapons to gain and maintain control and use of the electromagnetic spectrum. This signifies that any military action which uses electromagnetic energy and directed energy to disorganize, deceive, damage or destroy enemy use of the electromagnetic spectrum falls within the scope of electronic warfare. This theoretically greatly enlarges the operational sphere of electronic warfare and of its operational philosophy, illustrating that electronic warfare to "control the electromagnetic spectrum" has been "operationalized" and has been developed into a type of offensive military action. It is a major type of operation which runs through the entire process of modern high tech warfare and is also a major operational force element for winning victories. It can be used independently as a powerful force, or it can be combined with main force weapons, opening up a safe passage of attack for the main force weapons, producing a multiplier effect for the main force weapons. Therefore, offensive electronic warfare has developed into a fifth dimension battlefield after land, sea, air and space, breaking out of the traditional narrow operational philosophy of "self defense" and "defensive"

• The objective of electronic warfare is to weaken and destroy enemy overall combat capabilities

In the traditional concept of electronic warfare, ECM is used to prevent or to pre-weaken the enemy's effective use of the electromagnetic spectrum, and in the newly defined concept of electronic warfare, because of the use of destructive weapons of electromagnetic energy and directed energy, the targets of electronic warfare is no longer limited to attacking the electronic equipment and systems used by the enemy to transmit or receive radiational electromagnetic waves, but through the direct attack of enemy personnel, facilities and equipment, achieve the overall goal of weakening, disorganizing and destroying the enemy's overall combat effectiveness. This indicates that electronic warfare theory and operational philosophy has developed to a new stage. Electronic warfare is part of national overall strategy, and as high technology is converted to weapons and military equipment at an accelerated pace, a new strategy will be formed in the 21st century centered around electronic warfare. Electronic warfare capabilities have already become the key factor directly affecting modern weapons systems and the overall composite operational capability of overall military systems, as well as the key factor determining the progress and outcome of wars.

• Electronic warfare is the key element for the success or failure of command and control warfare

The newly defined C^2W is a fusion of electronic warfare with military deception, operational security, psychological warfare and physical destruction, their comprehensive application and close coordination, making every effort to oppose the enemy's overall command and control system including personnel. The primary task is to launch an active assault on the enemy's overall information

system in order to cut off the enemy command and control from his operational main forces, thus paralyzing the enemy forces and preventing the various enemy military forces from assembling, and making it impossible for the enemy to bring any possible potential superiority to bear. Therefore, compared to C^3 countermeasures strategy, C^2W includes more actively aggressive in nature and less reactive. First, it stress that in modern warfare, the destruction of the enemy command and control capabilities is a key and primary mission of every military action. Second, it considers the important role of people in command and control, thus making targets of the "senders" and "receivers" in the transfer of information, thus introducing psychological warfare with its broadcasting and dissemination of leaflets in order to break the will of the enemy forces into C^3 countermeasure strategic elements, constituting the five major supports of C^{2W} which are used all together. This is more powerful than the simple addition of the various strategic elements of C^3. Third, It uses aggressive electronic warfare in place of ECM, thus more closely fusing electronic warfare with C^2W, becoming the most important method used in CW strategy. Therefore, looking at the targets of their operations, C^2W and electronic warfare both have as their primary objective the damage of destruction of enemy command and control. Looking at the operational methods, key elements of electronic warfare operations such as electronic jamming, electronic deception, electromagnetic energy and directed energy attacks, signals security and radiation control as well as electronic psychological warfare which undermines the enemy's will to fight are all the most effective and most important component parts of the five major supports of C^2W. From the overall operational process of C^2W, the electromagnetic frequency spectrum ties the various spaces of modern warfare together, and has become the "fifth medium" of modern warfare. In the modern high tech battlefield, the collection of intelligence, the detection of

targets, the tracking, recognition and locating of targets, weapons control and guidance, and even operational decision making, issuing of operational orders and the evaluation of the results of operations all require the effective use of the electromagnetic spectrum. Therefore, attacks using electronic warfare weapons to attack any weak link in this cycle can bring the entire enemy war machine to a halt. Because electronic warfare with its objective of gaining and making use of the control of the electronic spectrum is a type of offensive military action, it becomes a core component part among the key elements of C^2W military strategy. Gaining control of the electromagnetic spectrum is the key to success in C^2W, so it is also a key to having all military actions proceed smoothly.

Clearly, the newly defined electronic warfare and C^2W have positions of increased prominence in high echelon military agencies. The memorandums of the United States Joint Chiefs of Staff demand that electronic warfare be more closely tied in with the establishment of operational headquarters, and require that offensive electronic warfare be more fully included in the operational plans of tactical commanders as a major component of modern warfare. In their operations, headquarters at all levels will establish formal C^2W organs, and joint electronic warfare centers will send personnel to reinforce the electronic warfare staff organs within joint command and expeditionary force staff organs. Headquarters will all make C^2W a central element while drafting operational plans.

Conclusion

In summary, because modern command and control systems and weapons control and guidance systems are all closely tied in with the electromagnetic spectrum, in modern high tech regional wars,

all participants must pay a great deal of attention to gaining control and use of the electromagnetic spectrum, because gaining so electronic warfare the purpose of which is to gain "control of the electromagnetic spectrum" has become an important offensive military action which runs through the entire process of modern high tech regional wars. At the same time it is also a crucial element of combat force in winning high tech regional wars. Therefore, since the electromagnetic battlefield was first established, this electronic warfare which can be neither seen nor felt has constantly developed, and along with it there has been formed a fairly complete operational philosophy of electronic warfare. A few of major viewpoints are:

• The electromagnetic spectrum occupies a special role and position in high tech regional wars and gaining control of the electromagnetic spectrum is the same as gaining the initiative of the "controlling heights".

• Electronic surveillance is prerequisite and precondition for conducting electronic warfare and other operational actions. Electronic intelligence is a huge, amorphous combat force.

• Electronic warfare has been elevated to a type of offensive military action. Its operational targets are not limited to the different types of military electronic equipment, but its objective is the weakening and destruction of the overall enemy combat strength. Therefore, one's electronic warfare capabilities are keys in determining the progress and outcome of wars. Traditional wars of large scale destruction which used the formula of fire power + mobility will give way to wars where victory is determined by the formula of "electronic warfare + fire power + mobility".

• C^2W is operational action closely tied in with electronic

warfare. In a strong electronic countermeasures environment, electronic warfare is the central component part of C^2W and the key to success or failure.

NAIC-ID(RS)T0398-96

NEWLY DEVELOPED CONNOTATIONS OF ELECTRONIC WARFARE UNDER CONDITIONS OF HIGH TECH WARFARE

BY: Ju Lianyuan

(Ministry of Electronic Industries, Institute 29)
(P. O. Box 429, Chengdu, Sichuan 610036)

ABSTRACT

This article analyses and explains the developments in a few areas of the connotation of electronic warfare following the Gulf War. From one on one equipment countermeasures, it has developed to system countermeasures. From only soft kill it has developed to a combination of soft and hard kill, to a combination of electronic warfare weapons and main combat weapons. From a single piece of equipment and small systems it has developed into a comprehensive electronic warfare system. From support measures it has developed into an offensive weapon. The new and expanded concept of electronic warfare. The mutual reliance between command and control warfare and electronic warfare.

During the Gulf War, high technology electronic weapons defeated traditional fire power and human weapons. Silicon chips defeated steel plate. We can predict from this that wars between high tech electronic weapons - electronic warfare, will become a primary form of high tech wars. Electronic warfare will be more widely used in future wars, thus promoting new developments in the connotations of electronic warfare. Following the Gulf War, the new developments in electronic warfare have primarily been in the following aspects:

1. Electronic warfare has developed from a one on one confrontation between pieces of equipment to system confrontation with the objective of weakening and destroying the enemy's combat effectiveness

Traditional electronic warfare is a one on one confrontation between pieces of equipment such as a jammer suppressing a radar or a radio. This type of electronic warfare is carried out by relatively dispersed and isolated operational elements and is fairly effective. Because of the lace of close contact between these operational elements, should one of these elements be jammed or suppressed, this element would stop functioning. However, on the modern battlefield, different radars overlap in their detection spaces and detection signals overlap. Different radios are connected in networks, communications signals can be carried over many different types of channels and circuits. The spaces defended by different guided weapons overlap, and guidance signals are relayed between them. For such modernized radar networks, communications networks and weapons guidance networks, traditional one on one electronic countermeasures almost have no effect. In order to remedy this it is necessary to develop system countermeasures and to have electronic warfare equipment directed at operational targets which not only include such military electronic equipment as radars, communications, guidance, IFF and computers, but also include the operators of the equipment and the operational commanders. The purpose of electronic warfare is not only to reduce or destroy the operating capability of the enemy's electronic equipment, but is also to weaken or destroy the enemy's combat effectiveness.

2. In system countermeasures, electronic warfare has developed from only soft kill (electronic jamming) to comprehensive countermeasures of a combination of soft and hard kill and a combination of electronic warfare weapons and main force weapons.

During the Gulf War, the Multinational Forces used innovative electronic warfare technology, changing the form of electronic warfare operations from the electronic jamming of the past to a combination of electronic jamming (soft kill) and anti-radiation missile attacks (hard kill), combining electronic attacks and destruction by hard weapons (missiles, bombs and shells). They concentrated their forces to attack the key weak links in Iraq's command and control such as the detection radars and communications centers. They also proposed the new concept of command and control warfare (C^2W). Electronic warfare is an important mainstay of command and control warfare, and command and control warfare is a major objective of electronic warfare. These two new combination methods in electronic warfare applications have manifest a new philosophy where the purpose of electronic warfare is to weaken or destroy combat effectiveness.

3. To meed the needs of system countermeasures, electronic warfare equipment has developed from a single piece of equipment or a small system to a comprehensive electronic warfare system composed of multiple platforms and multiple methods.

Traditional electronic warfare was often carried out between single pieces of equipment or small systems. The number of pieces of equipment being used was small, there were a few methods used, and each had a single function. Therefore, electronic warfare equipment design usually concentrated on how good the capabilities were of a single piece of equipment, and there was no need for further considerations. However, in system countermeasures, even if the capabilities of a single piece of equipment is very weak, it might still have very good operational effectiveness. For example,

a wide band, high power ECM aircraft is an expensive method of electronic attack. It is a powerful means of suppressing traditional early warning detection radar and communications radios. However, its operational effectiveness is very limited against modern air defense systems. Because the defenders can use high speed frequency hopping and band division to spread the jamming energy over the width of the spectrum, and can use super low sidebeam reception and spacial division to force the jamming signal energy to have increased dispersion range and selectivity in space. They can also use passive direction finding to get a fix on the jamming aircraft and guide anti-radiation missiles or other weapons in an attack on these aircraft. Therefore, in system countermeasures, it is necessary to use a number of types of electronic warfare operational platforms and a number of electronic warfare operational measures under the coordination and control of the operations command center to form an omnidirectional, large space, multiple frequency band, multiple method comprehensive electronic warfare operational system, that is, a comprehensive electronic warfare system. The comprehensive electronic warfare system is a new design concept for electronic warfare equipment proposed after studying the experiences of modern warfare and especially the experience of the Gulf War. It is the design philosophy for a new model of electronic warfare weapons system which has comprehensive system design, multiple use of signals, comprehensive resource management and control and which carries out composite countermeasures.

4. Electronic warfare equipment has developed from single platform support measures primarily self defense to an offensive weapon for attacking the crucial weak links within the enemy command and control systems.

Looking at the annual issue of "Jane's Weaponry", the vast majority of electronic warfare equipment is airborne and shipborne

self defense electronic warfare equipment. Traditional electronic warfare equipment are primarily targeted against precision guided weapons with a primary mission of serving as a part of a platform's self defense. Therefore, traditional electronic warfare equipment is a type of self defense support. During the Gulf War, the Multinational Forces shifted the emphasis of electronic countermeasures from the self defense of the operational platforms to electronic suppression and anti radiation destruction of Iraq's detection radars, communications centers and operational command centers. They also used electronic warfare weapons in conjunctions with main force weapons such as aircraft and ships, concentrating their forces to suppress enemy air defense capabilities and operational command capabilities so that the electronic warfare equipment developed from an operational support measure into an offensive weapon.

5. Updating and expanding the concept of electronic warfare

The gulf war triggered innovations and developments in electronic warfare technology and tactics. The use of new electronic warfare technology and new tactics led to new developments in electronic warfare concepts.

In March of 1992 the United States Joint Chiefs of Staff assembled the electronics warfare experts of the joint commands and special commands of the united states armed forces for a symposium on electronic warfare and made the decision to redefine the concept of electronic warfare[1].

The redefined electronic warfare includes the following three portions[2]:

- Electronic attack

This is the offensive portion of electronic warfare. It includes the use of electronic jamming equipment, anti radiation weapons, directional energy weapons and electronic deception methods to attack and deceive enemy personnel, equipment and facilities in order to reduce, inhibit and destroy enemy military effectiveness. Electronic attack places more emphasis on permanent damage and destruction of enemy electronic sensors than traditional ECM, so it is more offensive in nature.

• Electronic warfare support

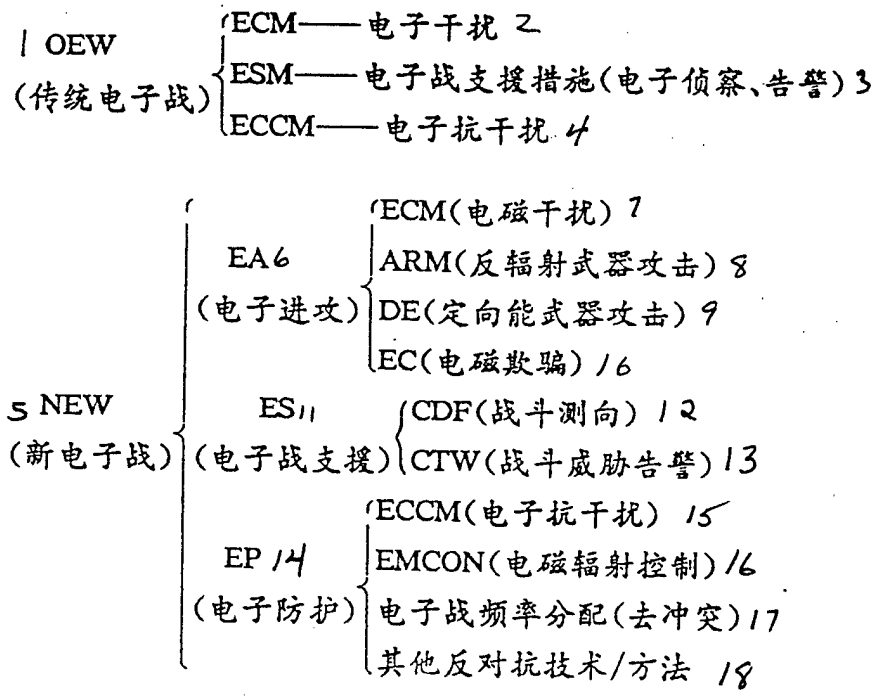
This is the use of electronic warfare surveillance equipment under the authority or direct control of commanders to search for, intercept, recognize, locate and recognize the direct threat of enemy intentional or unintentional radiations of electromagnetic energy in support of electronic warfare operations and other tactical actions (such as threat avoidance and homing, tracking and attack). Electronic warfare support places more emphasis on the comprehensive use of electronic surveillance and intelligence and other intelligence resources than traditional electronic warfare support measures in order to provide commanders with more and more accurate tactical intelligence support.

• Electronic protection

This is the defensive portion of electronic warfare. It includes ECM jamming, jamming of the enemy electronic surveillance equipment and other electronic countermeasure technologies and methods in order to prevent ones own personnel, equipment and facilities from being subjected to damage or harm from enemy or friendly electronic warfare. Electronic warfare protection provides more protection to ones own electronic warfare than traditional electronic counter countermeasures (ECCM), and the

strategy of attacking enemy electronic surveillance equipment in order to protect one's own electronic actions.

Fig. 1 Comparison of traditional and newly defined electronic warfare



1. Old Electronic warfare. 2. Electronic countermeasures. 3. Electronic warfare support measures (electronic surveillance, warning). 4. Electronic counter countermeasures. 5. New electronic warfare. 6. Electronic attack. 7. Electronic countermeasures. 8. Anti radiation missile attack. 9. Directed energy weapon attack. 10. Electromagnetic deception. 11. Electronic warfare support. 12. Combat direction finding. 13. Combat threat warning. 14. Electronic protection. 15. Electronic counter countermeasures. 16. Electromagnetic radiation control. 17. Electronic warfare frequency assignment (elimination of conflicts). 18. Other counter measure technologies/methods.

A comparison of traditional electronic warfare and the newly defined electronic warfare is shown in Figure 1. The newly defined concept of electronic warfare place anti radiation weapons and

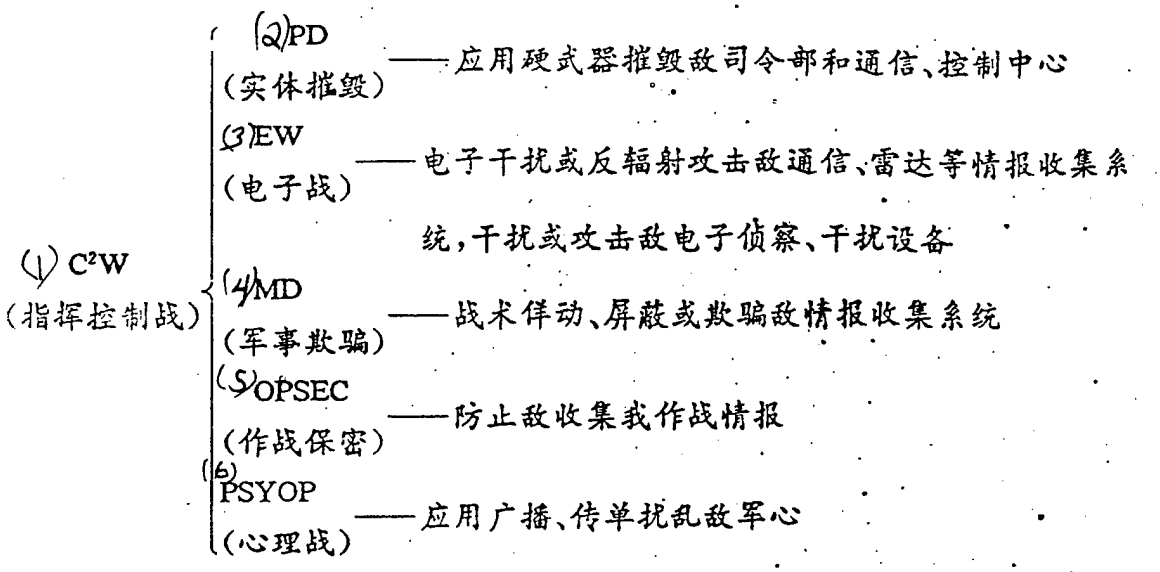
directed energy weapons within the scope of electronic warfare thereby increasing the offensive nature of electronic warfare, with electronic warfare developing from a role of strictly self defense support to a major operational measure which combines soft and hard kill, and has both offensive and defensive capabilities. At the same time, electronic protection not only considers protection against enemy electronic warfare, but also considers protection against friendly electronic warfare. Therefore, the new definition of electronic warfare is more suited to the characteristics of the modern battlefield and to the requirements of system countermeasures.

6. Mutual reliance between C^2W and EW

In March of 1992 the United States Joint Chiefs of Staff Operations Electronic Warfare Symposium held that "Desert Storm" demonstrated that command, control and communications countermeasures (C^3CM) are of increasing importance, but special emphasis should be placed on countermeasures against the command and control links of potential enemies. For this reason they suggested that C^3CM be changed to command and control warfare (C^2W)[1].

Command and control warfare (C^2W) is the comprehensive use of physical destruction, electronic warfare, military deception, operational security and psychological warfare with intelligence support to attack the overall enemy communications system including personnel in order to disrupt, reduce and damage enemy command and control capabilities while at the same time protection our own command and control capabilities[2].

Fig. 2 The five major mainstays of command and control warfare



1. Command and control warfare. 2. Physical destruction - the use of hard weapons to destroy enemy headquarters and communications and control centers. 3. Electronic warfare - Electronic jamming or anti radiation attacks on enemy intelligence collecting systems such as communications and radars, jamming or attacking enemy electronic surveillance and jamming equipment. 4. Military deception - tactical ruses to screen or deceive enemy intelligence collection systems. 5. Operational security - preventing the enemy from gathering intelligence on our operations. 6. Psychological operations - the use of broadcasting or distributing leaflets to disrupt enemy morale.

The contents of command and control warfare are shown in Figure 2. The changing of the traditional command, control and communications countermeasures (C^3CM) to command and control warfare (C^2W) is an indication of the high degree of attention the military has placed on attacks on command and control systems and their belief that C^2W is an important part of the operational plan drafted by commanders. The united States elevation of C^3 countermeasures to command and control warfare first took into consideration of the role of the individual in command and control,

thus expanding psychological warfare's use of broadcasting and distributing leaflets to disrupt the morale. Second, they placed additional stress on the soft kill (electronic jamming) and hard kill of the enemy's overall intelligence gathering system including communications and radars. Third, they stressed the combined use of physical destruction, electronic warfare, military deception, operational security and psychological warfare against enemy command and control as well as to protect their own command and control.

Based on the contents of the newly defined electronic warfare and command and control warfare, we can see that the following relationships exist between C^2W and EW:

• Electronic warfare is an important mainstay of command and control warfare, and command and control warfare is a primary objective of electric warfare.

• Electronic warfare is closely combined with other operational actions in order to attack the key links in the enemy command and control.

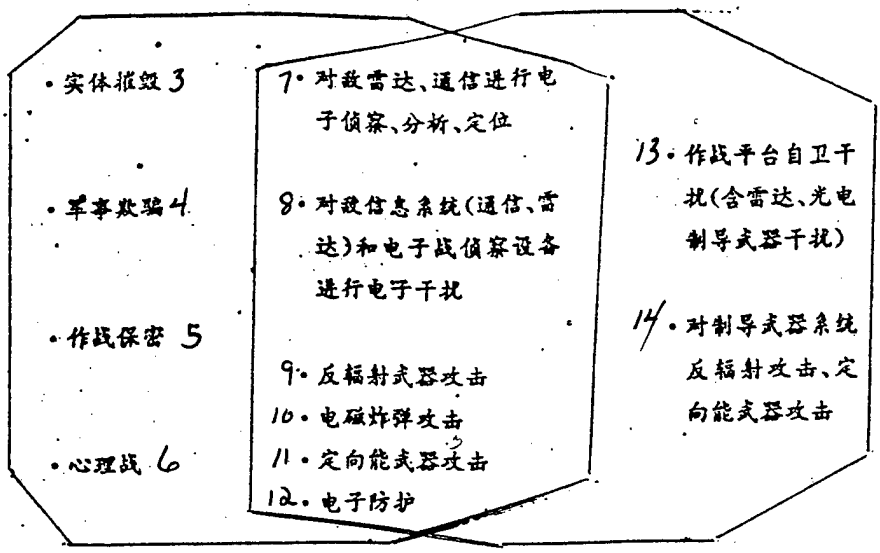
In modern warfare, the use of electronic surveillance and other surveillance methods to obtain electronic intelligence (ELINT), signals intelligence (SIGINT) Image intelligence (IMINT) and Human intelligence (HUMINT) in order to understand the enemy electronic weapons' operational sequence and the arrangement of the command and control centers provides command and control warfare (C^2W) with reliable intelligence support. Based on this intelligence data commanders select operational objectives and use hard weapons to destroy and electronic warfare soft and hard kill methods to attack operational command centers rendering them unable to form comprehensive attack forces or comprehensive defensive

forces, completely destroying the enemy operational command capabilities. In this process electronic warfare often precedes and follows up hard weapon attacks and runs through the entire process of operations in order to ensure our main battle weapons possess fairly high attack success rates and fairly low combat loss rate. Therefore, electronic warfare equipment and systems are multipliers of military force. They are the protectors of life and fortunes. They are primary mainstays of command and control warfare.

The relationship between command and control warfare and electronic warfare methods is shown in Figure 3. They are fused together and support each other.

We can see from the analysis above that following the Gulf War the concept, contents, equipment design philosophy of electronic warfare and the operational use of this equipment has all been updated and expanded, thus promoting electronic warfare to new heights, allowing even better use to be made of electronic warfare in high tech wars.

Fig. 3 The relationship between C^2W and EW



1. Command and control warfare. 2. Electronic warfare. 3. Physical destruction. 4. Military deception. 5. Operational security. 6. Psychological operations. 7. Electronic surveillance, analysis and locating of enemy radars and communications. 8. Electronic jamming of enemy information systems (communications and radars) and electronic warfare reconnaissance equipment. 9. Attacks using anti radiation weapons. 10. Attacks using electromagnetic bombs. 11. Attacks using directed energy weapons. 12. Electronic protection. 13. Self protection jamming by operational platforms (including the jamming of radars and optoelectronic guidance weapons). 14. Anti radiation attacks and directed energy weapon attacks against guided weapons systems.

BIBLIOGRAPHY

1. Gerald Green: "EW Transitions into the New World Order" JED 16(1), 1993. pp 15.

2. Jim Gray: "Turning Lessons Learned into Policy" JED. 16(10), 1993. pp 87-92.

NAIC-ID(RS)T-0398-96

THE DEVELOPMENT OF ELECTRONIC WARFARE THEORY AND OPERATIONAL USE OF ELECTRONIC WARFARE IN HIGH TECH WARS

BY: Quan Shouwen
(General Staff Institute 54)

ABSTRACT

This article introduces the process of changes in the development of the concept of electronic warfare and the new concepts of electronic warfare and command and control warfare and the relationships between these two. It explains the differences between the old and new definitions. It discusses the changes in the operational philosophy of electronic warfare brought about by the proposal of the new definition for electronic warfare. It analyses the characteristics of electronic warfare in future high tech wars and the operational use of electronic warfare.

1. Introduction

The tremendous successes of the Americans in the Gulf War produced a great effect on electronic warfare. When wrapping up their experiences, the American military held that the concepts of electronic warfare and C^3 countermeasures which had been used for a number of years no longer conformed to the reality of modern warfare. Electronic warfare had undergone basic changes in operational philosophy, operational methods and weapons used. It was necessary to make some additions and some changes to these concepts. At a recently convened Joint Chiefs of Staff meeting electronic warfare was redefined and C^3 countermeasures was changed to "command and control warfare". This change elevated the position of electronic warfare and expanded the capabilities included in electronic warfare. Stressing the offensive nature of electronic warfare increased the contents of electronic warfare, and basically changed the concept as it was understood by many

people that electronic warfare was "self defense" or "defensive". This change in the concept of electronic warfare indicates that electronic warfare has advanced to a new level, making the concept of electronic warfare more suited to the realities of modern warfare, and will affect the operational use of electronic warfare in future high tech wars.

2. Advances and changes in the concept of electronic warfare

2.1. Some electronic warfare concepts

The earliest definition of the concept of electronic warfare used by the United States military was: Electronic warfare is any military action using electromagnetic energy to determine, detect, weaken or impede the enemy use of the electromagnetic frequency spectrum and to ensure our own use of the electromagnetic frequency spectrum. It includes electronic support measures, electronic countermeasures and electronic counter countermeasures. Because surveillance, jamming and counterjamming are primary components of electronic warfare, and because in the beginning electronic warfare technology was extremely simple, it was understood by many in the military as a means of "self defense" or "defensive", and when commanders were considering overall problems, electronic warfare was merely a supplementary operational means.

In the middle seventies as anti radiation weapons became placed into use, especially with the onset of the confrontation between electronic warfare and the comprehensive air defense systems which relied on electronic systems, as well as the high capability military systems with their ever increasing reliance on electronic equipment being placed into use, long-held views concerning the electronic battlefield had to be reevaluated.

In the late seventies the United States military proposed the concept of "Combating the enemy operational command system" to supplement the narrow definition of "electronic warfare". "Combatting the enemy operational command system" was not merely conducting electronic suppression of enemy electronic equipment, but also included the use of fire power to destroy and seize these objectives.

With the formulation of the concept of C^3 (command, control and communications) systems, the term C^3 countermeasures came into being. At the same time a conceptual framework was established which included all necessary electromagnetic activity required in support of modern military actions. The United States Air Force established electronic combat (EC) as a concept. Electronic combat referred to all actions taken in support of military actions against enemy electromagnetic capabilities. Electronic combat included electronic warfare, C^3 countermeasures and suppression of enemy air defense systems. Electronic combat also included strikes against enemy electromagnetic capabilities and included protection of ones own electromagnetic capabilities. C^3 countermeasures referred to the comprehensive use of operational security, military deception, electronic warfare and physical destruction methods with the support of intelligence to prevent the enemy from obtaining information, and to influence, weaken or destroy enemy C^3 capabilities, while at the same time protection one's own C^3 system from threats of such actions. C^3 counter measures is composed of counter C^3 and C^3 defense.

In 1992 the United States Navy proposed a new theory of "Space Electronic Warfare (SEW), adding new contents to electronic warfare. The role of electronic warfare would be to cut off contact between enemy command and its units to create confusion within the enemy military and delaying enemy actions so the United

States forces would be able to achieve a quick victory with reduced casualties. Based on this new theory, the United States Navy requested comprehensive use of electronic jammers, radar homing missiles and electronic intercept systems to destroy the enemy C^3 network and deceive enemy intelligence sources, changing the defensive electronic warfare to an offensive electronic warfare.

2.2. New electronic warfare concepts and command and control warfare

We can see from all this that as science and technology and the level of weapons and equipment are further developed, there will be changes in the operational methods, operational spaces and operational styles used in modern warfare. The old concept of electronic warfare will no longer be fully reflect the electromagnetic actions of the modern battlefield, and additions must be made to the old concepts. In 1990 the United States Joint Chiefs of Staff published a definition of electronic warfare in MOP6 to replace the definition in MOP95. The new definition of electronic warfare added hard kill methods of "damaging" and "destroying" to the traditional ECM measures to prevent enemy use of the electromagnetic frequency spectrum, expanding the scope of electronic warfare. In March of 1992 the United States Joint Chiefs of Staff once more revised the definition of electronic warfare. This time they published two major policy papers MOP6 "electronic warfare" and MOP30 "command and control warfare" which redefined and delineated electronic warfare and renamed C^3 command and control warfare.

The new definition of electronic warfare was: Any military action using electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack enemy forces. There were three major components to electronic warfare: electronic attack,

electronic protection and electronic support. Electronic attack is the use of electromagnetic energy or directed energy to attack personnel, facilities or equipment for the purpose of weakening, inhibiting or destroying enemy combat capabilities. Electronic protection Electronic protection is the actions taken to protect personnel, facilities and equipment from any effects when our forces conduct electronic warfare or when the enemy uses electronic warfare to weaken, inhibit or destroy our combat capability. Electronic warfare support is the actions taken under the control of commanders to search for, identify and locate intentional or unintentional sources of electromagnetic energy emissions in order to immediately identify threats. The new definition of electronic warfare will include any military action which uses electromagnetic energy or directed energy to damage, deceive or destroy enemy use of electromagnetic waves.

Command and control warfare (C^2W), with the support of intelligence, is the comprehensive use of operational security, military deception, psychological operations, electronic warfare and physical destruction to prevent the enemy from obtaining information, and to influence, weaken or destroy enemy command and control capability, while at the same time ensuring that our own command and control capabilities are not affected by similar actions. Command and control warfare includes offensive and defensive aspects: Counter-C^2 and C^2-protection.

2.3. Comparing the new and old concepts of electronic warfare

Compared to the old definition of electronic warfare, a great many changes have been made to the contents of the new definition as are shown in Table 1. The new definition of electronic warfare include directed energy weapons and anti radiation weapons within the scope of electronic warfare, stressing the offensive nature and

hard kill properties of electronic warfare. In addition to considerations of protection against enemy electronic warfare, electronic protection also considers avoiding the effects of one's own electronic warfare.

Table 1. Comparison of contents of old and new definitions of electronic warfare

	1 包含内容	2 手 段
3 旧电子战	4 电子干扰	对敌雷达、通信、光电设备进行干扰 5
	6 电子战支援措施	电子侦察、告警 7
	8 电子反干扰	针对敌方干扰进行防护 9
10 新电子战	11 电子攻击	电磁干扰、反辐射武器攻击、定向能武器攻击、电磁欺骗 12
	13 电子战支援	电子侦察、威胁告警 14
	15 电子防护	电子反干扰(包括针对己方电子战的防护)、电磁辐射控制、电子战频率分配等其它反干扰措施。 16

1. Contents. 2. Methods. 3. Old electronic warfare. 4. Electronic jamming. 5. Jamming of enemy radars, communications and optoelectronic equipment. 6. Electronic support measures. 7. Electronic surveillance and warning. 8. Electronic counter countermeasures. 9. Protection against enemy countermeasures. 10. New electronic warfare. 11. Electronic attacks. 12. Electromagnetic countermeasures, anti radiation weapon attacks, directed energy weapon attacks, electromagnetic deception. 13. Electronic warfare support. 14. Electronic surveillance and warning of threats. 15. Electronic protection. Electronic counter countermeasures (including protection against one's own electronic warfare), electromagnetic radiation control, electronic warfare frequency allocation and other counter countermeasures.

Command and control warfare is a more thorough and complete concept built on the basis of C^3 countermeasures and the four

elements of C^3 countermeasures: Operational security, military deception, electronic warfare and physical destruction along with psychological operations, combining C^3 countermeasures and human factors, thus more fully combatting the overall enemy command and control system. Command and control warfare possesses the following characteristics: (1), it stresses the use of different methods to interfere with and destroy the overall enemy information system. (2), It includes psychological operations in command and control warfare, thus improving the effectiveness of C^3 countermeasures.

3. The significance of the electronic warfare concept

3.1. Changes in battlefield requirements reflected in the changes in the electronic warfare concept

The changes in the concept of electronic warfare have been influenced by battlefield requirements. The old definition of electronic warfare reflected the situation in the electromagnetic arena in the past. In the early days electronic warfare methods were simple and the targets were primarily a few radars. Therefore, even though electronic jamming was capable of greatly reducing the effectiveness of enemy radars, from the viewpoint of the overall situation, electronic warfare still occupied a position of secondary importance. After the seventies, a great deal of high capability military systems which relied on electronic equipment was constantly being placed into use, and the struggles in the electromagnetic arena became more complex, and more methods were used. The old concept of electronic warfare no longer reflected the overall situation of the struggles in the electromagnetic arena, so the United States military proposed a few theories, such as "combatting the enemy operational command systems", to supplement the narrow concepts of "electronic warfare". Especially

after the Gulf War where the operational philosophy, operational methods and operational weapons of electronic warfare in modern warfare were displayed, demonstrating that electronic warfare was an important operational force, and which ran through the entire process of combat, and which served as a multiplier. Therefore, the new definition of electronic warfare was proposed based on the experiences in the Gulf War. This definition included the use of directed energy and anti radiation weapons to gain control of the electromagnetic frequency spectrum and to dictate the use of the electromagnetic spectrum. This basically eradicated the mistaken notion of many that electronic warfare was "self defense" and "defensive".

The proposal of command and control warfare was also influenced by the Gulf War. The Gulf War made it clear that command, control and communications countermeasures (C^3 countermeasures) had become increasingly important, but that the emphasis should be placed on countermeasures against the enemy command and control systems. C^3 countermeasure methods and concepts were too narrow, and were excessively directed at equipment countermeasures. During the Gulf War, general Schwartzkoff combined the four traditional elements of C^3 countermeasures (operational security, military deception, electronic warfare and physical destruction) with psychological warfare, and attacking the overall Iraqi information system (including human factors) with unprecedented speed with tremendous success. The combination of C^3 countermeasures and psychological warfare elevated C^3 countermeasures to command and control warfare. Although psychological warfare is nothing new, and can play a role when used alone, when combined with C^3 countermeasures and when these five actions are coordinated they can maximize the effects of command and control warfare, thus launching an all out attack on the enemy overall command and control system.

3.2. The new definition enhances the position and contents of electronic warfare

In the Gulf War, the outstanding operational successes of electronic warfare illustrates that the theories and applications of electronic warfare have been developed to a new stage. Electronic warfare has become a fairly independent combat force in modern warfare. It has become a mainstay of modern warfare. The new definitions of electronic warfare and command and control warfare have markedly enhanced the positions of electronic warfare and command and control warfare. The United States Joint Chiefs of Staff memos required that commanders at all levels establish formal command and control warfare organs and that when headquarters were drafting operational plays command and control warfare should be a key element. The United States military holds that "Today, it is especially important to destroy the enemy command and control systems."

In modern high tech wars, command communications, weapons control, target surveillance and intelligence collection is all done by using the electromagnetic frequency spectrum. Therefore, control of the electromagnetic spectrum is the key to victory in command and control warfare. It is also the key to success in military actions. Therefore, electronic warfare is an important mainstay of command and control warfare, and is also one of the keys to victory in modern warfare.

The new definition of electronic warfare gives electronic warfare much more of an offensive nature. It provides electronic warfare with kill capability. In the 1990 revised definition of electronic warfare, "damage" and "destruction" were added, and anti radiation weapons were placed within the scope of electronic

warfare. Furthermore, the new definition also included anti radiation weapons and directed energy weapons within the scope of electronic warfare. According to this new definition, in addition to traditional electronic countermeasures, anti radiation missiles, anti radiation drones, high energy lasers and RF weapons are all methods of attack in electronic warfare.

This revised definition of electronic warfare includes the protection against damage from one's own electronic warfare in electronic protection, requiring electronic equipment to also prevent electronic interference from one's own forces while protecting against enemy electronic attacks. This reminds people to pay attention to electronic interference between units to prevent "accidental casualties" from electronic warfare.

3.3. Overall strategy is given prominence in command and control warfare, making even greater demands on intelligence and surveillance

By changing C^3 countermeasures to command and control warfare, the United States military has elevated it to the position of overall strategy. C^3 countermeasures only stressed equipment countermeasures, making it easy to confuse it with communications electronic warfare. After the addition of psychological warfare, C^3 countermeasures was elevated to command and control warfare, making the enemy's overall command and control system (including human factors) its operational target, and giving prominence to the overall situation. Modern warfare is a confrontation of system against system. The command and control system is the central nervous system of the overall operational systems, and the commander is the brain controlling the movements of the entire system. Command and control warfare defines its target as the command and control system. Its purpose is to paralyze the central

nervous system of the enemy's operational systems, collapsing the entire enemy war machine and at the same time ensuring that one's own systems operate normally.

Because the Multinational Force successfully damaged the Iraqi command and control system during their bombing raids during the Gulf War, it was almost impossible for President Hussein to exercise centralized control over his units, and regional commanders were unable to coordinate and organize effective defenses. Psychological warfare destroyed the morale of the Iraqi forces. To a great extent, then, the success of the Multinational Forces must be credited with the timely and coordinated conduct of command and control warfare.

In order to be effective, command and control warfare must be based on reliable intelligence from multiple sources. When drawing up the operational plans for command and control warfare, the determination of operational targets requires detailed, reliable intelligence support from a number of sources, including signals intelligence, human intelligence and image intelligence. During the process of conducting command and control warfare, the evaluation of operational results, damage estimates and the drafting the next operational plan all require reliable intelligence sources consistent with the progress of the operations to support the command and control warfare operations during each period. Therefore, command and control warfare makes even greater demands on comprehensive multiple source intelligence, and the reliability and timeliness of intelligence.

4. The operational use of electronic warfare in future high tech wars

The new theories of electronic warfare make even greater

demands on intelligence and surveillance, prompting greater attention on electronic intelligence and surveillance. Electronic intelligence and surveillance is divided into peacetime surveillance and wartime surveillance.

The methods used in electronic intelligence and surveillance are basically the same in peacetime and wartime. The only difference is the intensity. During time of peace electronic intelligence and surveillance long term surveillance and monitoring conducted against enemy electronic activity. The purpose of electronic intelligence surveillance is not only to monitor such parameters as the frequencies and azimuth of electronic equipment in preparation for jamming, but is also to use surveillance, determination of enemy strategic and campaign targets and to determine the parameters of electronic equipment which can be used for operational planning for aircraft guidance and precision guided weapon attacks as well as for electronic countermeasures. Peacetime electronic intelligence and surveillance is relatively fixed and regular. Peacetime electronic intelligence and reconnaissance is a primary basis used in the drafting of electronic warfare operational plans and for drafting electronic equipment development plans.

Reconnaissance measures primarily include: Electronic reconnaissance satellites, reconnaissance aircraft, reconnaissance vessels, drones, and ground reconnaissance stations. Satellites will be come the primary method of electronic intelligence and reconnaissance and for transmitting intelligence.

4.2 The first operation is the use of electronic suppression to gain control over the electromagnetic frequency spectrum

4.2.1. Electronic warfare has become the prelude to modern warfare,

and has developed into an independent operational stage

The traditional formula for joint operations: air raids and air defense confrontation (gaining control of the skies) - surface offensive and defensive warfare (decisive battles). Operations under current conditions are: electronic warfare (gaining control of the electromagnetic spectrum) - air raids and air defense confrontations (gaining control of the skies) - surface offensive and defensive battles (decisive battles. Furthermore, electronic warfare runs from the beginning to the end of the combat. The electronic warfare in the initial operations has become an independent operational stage that cannot be replaced by any other combat force.

4.2.2. Placing stress on a blanketing electronics attack while gaining electromagnetic superiority.

This is conducting overall, total spectrum, and in-depth electronic suppression with the support of electronic surveillance. There are hard and soft types of electronic attack suppression. Soft suppression is carried out using electronic countermeasure aircraft and ground jamming stations. Hard suppression methods include anti radiation weapons, directed energy weapons and some conventional missiles and bombs.

Aerial platforms are an increasing proportion of the equipment used, helping to increase the effective range and mobility and achieving multiple directional and in-depth suppression, and also helping to coordinate with the second stage attacks.

In the opening stages of the war, the primary targets of electronic warfare attacks will be enemy command and control systems, stressing the use of hard kill methods (including anti

radiation weapons and conventional hard kill weapons, and even directed energy weapons) to strike enemy command and control centers and fire control systems along the line of attack in order to clear the way for the attacking aircraft.

4.2.3. The confrontation between precision guided weapons and AWAC aircraft will become an important part of electronic warfare countermeasures

When the war first begins, the use of large numbers of precision guided missiles will unavoidably lead to a precision guided missile confrontation between the offensive and defensive sides. An important part of this will be optoelectronic countermeasures.

The reliance on AWAC aircraft in the air war will also make the AWAC aircraft key targets of attack. It is possible that airborne jammers will be use to jam the radars and communications of the AWAC, or that missiles (including long range anti-radar missiles or other missiles) will be used to attack the AWACs. There are reports that the Russians have developed a passive radar guided missile which can destroy AWAC aircraft at long range.

4.3. Electronic warfare equipment capabilities and functions will be further enhanced

4.3.1. The attacking formations will require close coordination with ECM aircraft

In future wars it will be required that ECM aircraft closely coordinate with combat aircraft (including coordination between aircraft of different services) in order to make best use of electronic warfare aircraft. ECM aircraft will be used in the following ways:

A. Long range support jamming beyond the theater

This will usually be done by ECM aircraft from a number of directions, and they will often be joined by ground jamming equipment in order to make the jamming more effective. The targets of the jamming will be enemy C^3I systems and early warning systems, forming a jamming screen which will screen the combat aircraft in their attacks.

b. When large groups of aircraft are penetrating enemy defenses, anti radar aircraft will open a path for the attacking aircraft and ECM aircraft will follow the group to conduct jamming support

Composition: Ordinarily there will be between 20 and 40 main attack aircraft in a formation with four to six fighters flying escort, two to four anti radar aircraft opening up a path, and around four ECM aircraft providing Jamming support outside the formation.

The anti radar aircraft will use anti radiation weapons to attack radars (including air defense weapon control radars) along the flight path of the attack, and they may supplement this with attacks by weapons with other types of guidance. When the attacking formation breaks through enemy defenses, helicopters will often be used to assist in anti radar attacks.

C. Small formation operations will have the jamming support of one ECM aircraft.

In future air battles, as aircraft mobility, single aircraft fire power and airborne electronic equipment capabilities are all enhanced, small formations will be used more often in attacks of

multiple layers, multiple sorties and from multiple directions. At such times ECM aircraft will follow the attacking formation conducting jamming support, and upon arrival at the target area it will provide support outside the range of fire power.

These three methods of jamming support will frequently be used at the same time in order to achieve total depth, multiple directional suppression.

We can see from the discussion above that ECM aircraft will have to constitute between 15 and 20 percent of the attacking aircraft in order to ensure sufficient jamming support capabilities.

4.3.2. Airborne self defense jamming capabilities will be further enhanced

As air defense fire power continues to become stronger, additional requirements will be made on airborne self defense ECM capabilities. Following the Gulf War, the United States made the following summarization: The airborne self defense ECM capabilities current possessed by the United States can only satisfy 25 percent of operational requirements. Whether or not this is correct, we can see from the current developments in United States equipment, airborne self defense ECM equipment is being targeted for development.

The requirements for self defense ECM equipment is multiple functions in a single piece of equipment, stressing increasing warning capabilities and self adaption capabilities. In future wars, some combat aircraft will be equipped with anti radiation missiles for self defense so combat aircraft will possess soft and hard kill self defense capabilities.

4.3.3. Vehicle carried equipment will have better mobility

Vehicle carried equipment needs to have better mobility in order to adapt to the characteristics of modern warfare of high speed and flexibility. Many pieces of equipment will be used on aerial platforms rather than vehicular platforms.

4.4. Hard kill weapons will be more widely used

4.4.1. Anti radiation weapons

Anti radiation weapons are primarily composed of anti radiation missiles, anti radiation drones and anti radiation shells. Anti radiation weapons are a primary hard kill tactic in electronic warfare, and in future wars they will be very widely used. Almost 20 different types of anti radiation weapons have already been developed, to the third generation. Representative of the third generation equipment are the United States "Hamu" (phonetic) missiles and the English "Alamu" (phonetic) missiles. Around the year 2000 the third generation anti radiation weapons will still be used in large numbers, but some individual properties may be improved.

The types of anti radiation weapon attacks include:

A. Direct attack

This type refers to cruise or parachute attacks. It is a direct attack aimed at a predetermined target. The first commonly used method is for the carrier aircraft to enter at low altitudes, and then climb into the beam and launch the weapon. The other

method is for the aircraft to enter at low altitude and then launch the missile skyward. The missile will climb at a predetermined sequence, enter the wave beam and then attack.

b. Cruising and parachute, lurking attacks

Anti radiation drone aircraft cruise and search after they are launched, and there are a number of anti radiation missiles such as the "Alamu" (phonetic) missile which after launch climbs, and then deploys a parachute after reaching the top of its trajectory, and searches during its slow fall. After these types of anti radiation weapons locate a target, they attack the predetermined priority target. They may also select lower priority targets for attack. This is a capability even more complex.

C. Attacks in coordination with the use of decoys

A drone is first launched as a lure to trick the radar into being turned on, and then an anti radiation weapon carrier aircraft launches an anti radiation weapon at the radar.

D. In coordination with other methods

This is the use of other missiles (such as television guided missiles) in supplemental attacks when using anti radiation weapon attacks.

4.4.2. Directed energy weapons

With the broadened definition of electronic warfare, directed energy weapons such as lasers, RF weapons and ion beam weapons all fall within the scope of electronic warfare. Because directed energy weapons are very powerful and have a small area of

destruction, this helps to control the degree of the strike, and they do not leave any toxic "residue". Therefore, there is not the same reluctance to using directed energy weapons as there is to using such things as nuclear weapons.

Of the directed energy weapons, the laser weapons are the most developed. By the late eighties there were already a number of experimental prototypes of close range tactical laser weapons. It is predicted that by the year 2000 armed forces will be equipped with a small number of tactical laser weapons. The United States began research into using high energy electromagnetic pulses generated by explosions in electronic warfare. The technology for this is now mature.

Because directed energy weapons are subject to power source and technology limitations, they will not be able to be used as widely on the battlefield as anti radiation weapons. They will only serve as a future type of weapon for electronic warfare. However, with the new definition of electronic warfare, this will promote the development of directed energy weapons. Therefore, a problem to be considered in developing electronic equipment will be electromagnetic hardening to reduce the amount of damage from directed energy weapon attacks.

4.5. The role of stealth aircraft

before and after the year 2000, stealth aircraft will continue to be primary means of attacking major targets deep within enemy territory. Stealth aircraft usually have their own formations, and may use cover provided by long range support jamming. During their attacks stealth aircraft will generally maintain radio silence, and penetrate target airspace undetected. They will use precision guided missiles at close range to destroy targets. Other combat

aircraft will usually follow stealth aircraft after their attacks to provide escort. During the Gulf War, a formation of about 10 American F-117A stealth aircraft made the initial raid of crucial targets and F-15 aircraft penetrated target airspace about five minutes later for follow up raids and to provide escort.

Because of their high cost and complex technology, stealth aircraft cannot be manufactured in large numbers to equip units. From the viewpoint of their operational use there is no need for them to be used to equip units in large numbers for the short run. Around the year 2000 there will still only be a few major countries which will be equipped with stealth aircraft. Smaller nations will probably not be equipped with them. Even for a superpower like the United States, only a small percentage of their combat aircraft are stealth aircraft. By the year 2001 the United States will only have 57 F-117 aircraft and 20 B-2 bombers, less than two percent of the total number of combat aircraft. Even when the F-22 is placed in service in the year 2005, stealth aircraft will only be 10 percent of the total number of combat aircraft. America's air forces will be formed by a mixture of stealth and conventional aircraft.

Although units are equipped with only a small number of stealth aircraft, they have an obvious role which was made very evident during the Gulf War. Advanced stealth aircraft are not only an important means of attack, they can also be viewed as a deterrent force.

4.6. Some tactics in electronic warfare

As electronic warfare has developed and been widely used, a number of tactics have appeared which are related to electronic warfare, such as electronic feigned attacks, electronic deceptions,

radio silence, etc. The operational applications are as follow:

A. Providing cover for unit attacks

Many future wars will be short lived and quickly decided by raids. The strategic targets cannot be concealed, but through the use of electronic feigned attacks and deception, it will be possible to conceal the direction of the attack, and timing of the attack and the scale of the attack to achieve the element of surprise and to achieve suddenness in the campaign.

Also, during their attacks, stealth aircraft often use radio silence in order to attack undetected.

B. Providing cover for unit mobility

In modern wars, both sides frequently use surveillance of the activities of the other side to determine their actions. Therefore, radio activity (frequency, strength, etc) is controlled during operations to mislead the enemy and provide cover for unit moves.

C. Electronic warfare raids during operations

This is the sudden use of secret or new electronic warfare measures such as nuclear electromagnetic pulse to attack the enemy electronic equipment, incapacitating the enemy and achieving the objective of defeating the enemy. With the rapid advancements in science and technology, these electronic warfare tactics using new technology could appear in future wars.

D. There will be large scale use of camouflage and deception and decoy targets

In modern warfare there are increasing numbers of reconnaissance methods using increasingly advanced technology, so if targets are not camouflaged they will be easily detected. This means that they could easily come under attack and be destroyed. Therefore, in addition to stronger air defense fire power, another important measure in protecting important targets is the use of camouflage and decoy targets to increase the survivability of these important targets. Actual combat has demonstrated that such methods are effective, and that they are widely accepted. They will be used a great deal in future wars, especially in defensive operations.

When using these tactics, it is naturally necessary to have unified planning, unified management and coordinated actions. When using electronic warfare tactics against the enemy, coordination of one's own radars, communications and intelligence units must be emphasized in order to have electronic warfare tactics carried out smoothly.

BIBLIOGRAPHY

1. "U.S. Air Force Air and Space Campaign Regulations AFM2-8 - Electronic Warfare Actions", August 1 Publishing House, Jan, 1993.

2. Jim Gray, "Turning Lessons Learned into Policy", JED, 16(10), 1993, pp 87-92.

3. Jiao Jianxing, "The New Change In the U.S. Military Definition of Electronic Warfare", Electronic Countermeasures, 2, 1994.

4. Quan Shouwen, "A Description of Electronic Warfare in the Gulf War", internal document.

ELECTRO-OPTICAL COUNTERMEASURE TECHNOLOGY FOR GUIDANCE STATIONS (OR PROTECTED TARGETS

B: Ji Shiao

(Second Academy, Department Two)

1. Use of electro-optical countermeasure technology in modern warfare

Electro-optical countermeasures referred to in this article primarily refers to countermeasure technology with the addition of the optical spectrum into the electromagnetic frequency spectrum. Since the sixties electro-optical technology such as television, lasers and infrared have gradually become widely used in weapons for tracking, ranging, detonation, guidance and especially in precision guided weapons, spurring a corresponding development of electro-optical countermeasures. The struggle between countermeasures and counter countermeasures within the electromagnetic spectrum has become an important part of modern warfare. This holds true for countermeasures in the microwave spectrum and for the optical wave spectrum. Whoever wins this struggle will possess the initiative in combat.

The Vietnam War, the Middle East Wars, the Falkland Island War, the Soviet invasion of Afghanistan, the United States Raids over Libya, and the Gulf War "Desert Storm" all took place within the framework of electro-optical confrontation. The electro-optical guidance and counter guidance, reconnaissance and counter reconnaissance equipment used by both sides in a conflict has become increasingly complex and with an increasing of different types in increasingly large numbers. Furthermore, they are constantly being used in new ways. This has become a prominent characteristic of modern warfare.

In 1972 during the Vietnam War the North Vietnamese used Soviet SA-7 infrared guided missiles with an extremely high hit rate. After the initial shooting down several dozen of their aircraft, the Americans began adopting the method of dropping decoys which rendered the SA-7 missiles almost completely ineffective. Later, the Soviet Union improved its SA-7 missiles, adding an optical filter, which allowed the SA-7 top achieve good effects in the Fourth Middle East War. Then, Israel once more improved its countermeasures technology which permitted a great drop in its aircraft losses.

In 1986 the United States military conducted a surprise raid on Libya Because the operating frequencies of the Libyan combat weapons were concentrated on the microwave band, and Libya did not have electro-optical guided weapons and effective electro-optical countermeasure capability. The operating frequencies of the American weapons, however, were spread out over a wide frequency spectrum, and by conducting various types of radio jamming they rendered the Libyan surface-to-air missiles ineffective. They also used laser, television and infrared imaging electro-optical precision guided weapons in their attack. As a result, in one action then destroyed the Libyan surface facilities. The major reason for the Libyan loss was that they did not possess electro-optical countermeasures.

During the War in Afghanistan, between 1986 and 1987, the guerrillas got their hands on several hundred "STINGER" missiles with excellent electro-optical counter jamming capabilities. This allowed them to shoot down an average of 270 aircraft per year, at a loss of two billion U.S. Dollars, and the missiles only cost 60,000,000 U.S. Dollars, a ratio of 33 to 1.

In the 42 day Gulf War in early 1991, both sides used optical

countermeasures and counter countermeasures a great deal. This was optical electronic warfare of unprecedented scale. The result of this confrontation played an important role in the progress and outcome of the war. During the war, the Multinational Forces used composite formations made up of a number of different types of aircraft. In addition to EA-6B and EF-111A special electronic warfare aircraft with a great deal of electro-optical countermeasure equipment flying in these formations, the different combat aircraft were all equipped with various models of self defense electro-optical countermeasures devices such as the infrared ECM bombs RR-119, MK-46, MK-47, M206, MJU-7/B, MJU-8, AN/ALS-34 and AN/AAS-26; infrared jammers AN/ALQ-107, AN-ALQ-123, AN-AAQ-8(V), AN/ALQ-140, AN/QLQ-144, AN/ALQ-146 and AN/ALQ-157; and different models of chaff and infrared ECM bomb launchers AN/ALE29A, b, AN/ALE39, AN/ALE40, AN/ALE-45, M-130, AN/ALE-24 and AN/ALE-28. They were used to equip B-52 and F-111 bombers, A-4, 1-6, 1-7 attack aircraft, F-4, F-15 and F-16 fighters and AH-1 and CH-46 helicopter gunships. These electro-optical countermeasure methods effectively suppressed the Iraqi military SA-7-2SM, SA-9 and SA-13 "LUOLANTE"-2 (phonetic) electro-optical guided surface-to-air missiles during the Multinational air raids, with a loss rate of Multinational Forces military aircraft of only 0.5 percent, with the aircraft electro-optical self defense ECM measures playing an important role.

We can see from these examples that "electro-optical countermeasure" equipment actually plays a very large role in warfare. It requires that we pay a high degree of attention to it. China's strategy is one of strategic defense, and in future wars we will even more be in the position of fighting a defensive operation. With China's conditions, we must pay greater attention to the study of electro-optical countermeasure technology in the areas of protected targets on the ground. We must equip guidance stations and protected target zones with electro-optical

countermeasure equipment so they will be able to effectively carry out electro-optical countermeasures against operational equipment aboard enemy aircraft, especially precision guided weapons, to achieve the objective of "protecting ourselves and wiping out the enemy". This is also a problems which requires special attention by personnel conducting research on surface-to-air missiles.

2. Foreign developmental trends in electro-optical countermeasures technology

Electro-optical countermeasure technology is the counter countermeasure technologies which are used in optical detection, tracking, ranging, guiding and detonation, including optical countermeasure technology. That is, the two conflicting aspects of optical countermeasure technology and optical counter countermeasure technology. The developments in optical countermeasure technology have come about within this struggle between these two conflicting aspects. In the past few years optical precision guided weapons have become the mainstay in the development of precision guidance technology, and the corresponding optical countermeasure technology has become the object of widespread interest among the major nations, with investments in this technology increasing every year. After the eighties, the amount spend on research into optical countermeasure technology by the United States increased at a rate of around 21 percent a year, which is more than the 15 percent annual growth rate for microwave ECM. The primary direction of the development of electro-optical countermeasure technology is primarily the widespread use of infrared imaging detection, tracking and guidance technology, against which the previously effective countermeasures (infrared ECM bombs, infrared Jammers and smoke which was effective against shortwave) all pale by comparison. Under these conditions, it is necessary to develop new effective countermeasures against infrared

image guidance. At the present time the primary direction of developments have been in:

A. Active research into infrared medium and long wave smoke screens

Smoke screens which can act as countermeasures against visible light and near infrared is mature technology. The deployment of these types of smoke screens has already become a practical and effective passive countermeasure. However, this type of smoke screen is generally fairly ineffective against 3-5μm and 8-12μm medium and long wavebands. Therefore, it is necessary to develop infrared smoke screens which can jam medium and long wave infrared light sources as well as equipment to launch these smoke screens.

B. Development of new infrared decoys

Tracers are an effective infrared decoy shell, and have been widely used on the battlefield, and they are effective in jamming monochrome point source infrared guided missiles. They will continue to play a role on the battlefield for a certain time into the future. With the widespread application of thermal imaging guidance technology, it has been difficult for tracer rounds to perform a jamming function. Infrared decoys must also be developed from point source radiation toward plane source radiation, so they can form large area infrared radiation and cover targets, or form thermal images similar to the target being protected. During the 1991 Gulf War, Iraq erected plastic "Scud" missile launchers, fooling the infrared surveillance equipment of the Multinational Forces. These plastic launchers were mew model infrared decoys. They resulted in the multinational forces reporting the destruction of more "Scud" missile launchers than what Iraq actually possessed, and "Scud" missiles continued to be launched. This illustrates

that these plastic launchers served as a deception.

C. Development of suppressive active countermeasures

Countermeasures against infrared imaging guidance technology are currently concentrating on the development of laser blinding equipment. At the present time, laser beams are already capable of carrying a great deal of energy, enough to destroy infrared sensors, optical filters and modulation disks, as well as destroy the missile nose cone. Therefore it has become an effective measure for countering precision guided missiles. The U.S. Army "Hongyu" (phonetic) weapon is a mobile truck-carried "optical and electro-optical countermeasure system:. The Army calls the "Hongyu" (phonetic) a "low energy laser system". Its purpose is to damage the sensors of current generation optical precision guidance weapons. A prototype weapon was developed in 1986. In 1991 it was used to equip units. The United States Air Force has a similar development program called the "Crown Prince". In addition, the United States, the former Soviet Union, Germany and France are all actively developing tactical air defense laser weapons, primarily to be used against different types of tactical missiles. This type of laser weapon will be able to destroy the outer skin of he missile as well as destroying sensors and optical systems.

D. Infrared emission suppression and masking technology

The purpose of this is to reduce and eliminate the difference in infrared emission between a target and its background. Foreign countries have studied a number of measures for infrared suppression which reduce the infrared emissions of exposed metal outside of aircraft engines and the exhaust flame to very low levels. Using thermal masking mesh, thermal masking paint and thermal distortion camouflage paint not only can suppress the

intensity of the targets infrared radiation, but can also distort the thermal characteristics of the target, serving as jamming against infrared imaging guided missiles.

E. Research into countermeasures against infrared guided weapons

The current focus in the development of infrared imaging technology, imaging differentiation technology, application of doppler characteristics and variable field of view technology.

F. Unified equipment

Developments in the comprehensive use of countermeasures are tending toward unification in a single piece of equipment, universal use, making the equipment intelligent and making it multi-functional. Because the threat from the enemy is no longer a single form, this requires that countermeasure systems be capable of multiple mode operations. It must be capable of threat warning, enemy analysis, digital processing, optimum response selection, carrying out multiple types of countermeasures. For example, the British and French have jointly developed the "Sorceress" shipborne decoy launch system and the American Navy and Air Force have jointly developed the INEWS total spectrum electronic warfare system, both of which are unified electro-optical countermeasure equipment.

3. Guidance station (or protected target) electro-optical countermeasure technology

3.1. Operational targets of electro-optical countermeasures

Using the Gulf War which occurred in 1991 as an example, we will look at the current operational targets of air defense

electro-optical countermeasures.

During the Gulf War, the first weapons used were more than 100 ship-launched "Tomahawk" Cruise missiles accompanied with the launch of electronic warfare missiles. These missiles concentrated on attacking Iraqi air forces, surface defense forces, C^3I systems, etc. This was to temporarily or partially paralyze these targets to provide a safer environment for bombing by follow-up aircraft bombing raids. After the attacks by the cruise missiles, aircraft were used in air raids. At the forefront of the bombing raids were F-4G aircraft carrying high speed anti-radar missiles. When conducting air raids over targets which still possessed air defense capabilities, there were often high altitude or long range launches of precision guided bombs (including Stand-off laser guided bombs, etc) or launches of air-to-ground missiles AGM-65 (Maverick) or (Hellfire) missiles. During the air raids by the waves of aircraft, the Americans used a number of F-117A stealth aircraft, making full use of their characteristics of being difficult to detect by radar, their strong ability to penetrate defenses, and their suitability to long range bombing raids. It is said that the first guided bomb to hit Baghdad was launched by one of these.

We can see from all of this that in addition to aircraft continuing to be major air threat targets, cruise missiles, air-to-ground precision guided missiles (including anti radiation missiles), laser guided bombs and stealth aircraft have all become major targets for modern air defense weapons. The guidance systems used by missiles and bombs are primarily laser semi-active guidance, infrared imaging guidance, visible light television guidance and RF guidance.

3.2. Basic technology indexes of electro-optical countermeasure systems

A. Radar or infrared aircraft detection range of more than 10 km.

B. Radar or Infrared missile detection range of more than five km.

C. When an airborne laser is directed on a target at more than eight km, the laser beam can be detected near the target zone.

D. Detection angle range: Azimuth angle >90°, elevation angle of 45°.

E. Detection angle position accuracy ≤1°.

F. Detection wavebands: Infrared - 3-5μm, 8-12μm, laser - 1.06μm.

G. Detection precision for laser pulse repeat cycle is <2μs.

H. Detection precision for laser pulse width is 2ns.

I. ECM equipment set up time <1-2s.

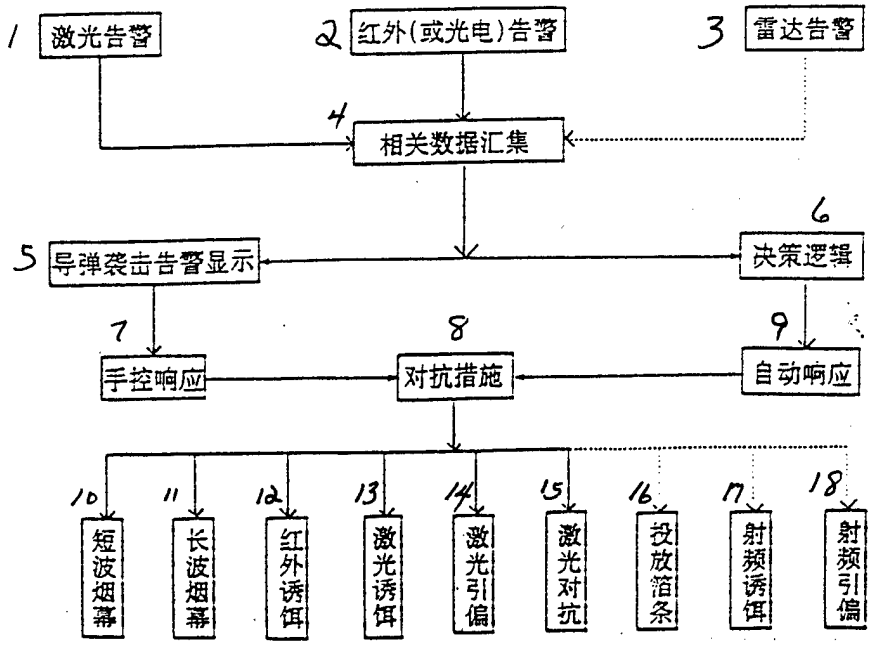
J. Capable of determining the property of incoming targets (aircraft or missile) and the type of guidance used by the missile.

K. Capable of effectively jamming television guidance, laser guidance and infrared guidance and different types of countermeasures.

3.3. Basic system composition and its capabilities

The basic composition of electro-optical countermeasure

systems is shown in the following figure.



1. Laser warning. 2. Infrared (or electro-optical warning. 3. Radar warning. 4. Coherent data assembly. 5. Missile attack warning display. 6. Decision logic. 7. Manual response. 8. Countermeasure. 9. Automatic response. 10. Short wave smoke screen. 11. Long wave smoke screen. 12. Infrared decoy. 13. Laser decoy. 14. Laser deception. 15. Laser countermeasures. 16. Dropping chaff. 17. RF decoy. 18. RF deception.

The equipment is primarily composed of three major parts: The first part is the warning equipment, including infrared warning, laser warning and radar warning. The mission of he infrared warning is to detect the infrared radiation and azimuth of incoming targets (aircraft or missiles). The mission of the laser warning is to detect laser radiation upon the protected target zone and to determine the azimuth, wave band, pulse width and repeat frequency of the laser radiation. For the radar warning, it is possible to use air defense system (or surface-to-air missile) advance warning radar. Each of the pieces of warning equipment send the signals

they detect to the central control computer. The second part is the central control computer. Its mission is the comprehensive analysis of the different information obtained by the warning equipment and to determine the type of incoming target, select the optimum countermeasure strategy, control the jamming procedure and to start up the jamming equipment. The third portion are the different types of jamming equipment, including rapid release smoke screen (including short wave smoke screens and long wave smoke screens), rapid release decoys including (infrared decoys, laser decoys and RF decoys), deception equipment (including laser semi-active guidance deception equipment and RF counter anti radiation missile deception equipment), laser blinding equipment (with further development can be used in conjunction with tactical air defense laser weapons).

4. Missile approach Warning (MAW)

Missile approach warning devices are primarily laser warning, infrared (electro-optical) warning and radar warning. Radar warning is primarily airborne early warning radar, RF jammers and airborne (or missile) guidance radar warning. It may be achieved by relying on ground early warning radar or guidance station search radar. It is not very effective against passive guidance or laser guidance weapons. Most air-to-surface missile guidance systems are infrared guidance and laser guidance. Incoming warning of these missiles relies primarily on infrared warning and laser warning.

4.1 Infrared (electro-optical) laser warning devices

Because electro-optical missile warning devices have excellent concealment properties and have a high degree of flexibility, after the Gulf War the United States has focussed its missile approach warning device development on electro-optical models.

1 型号	2 体制	3 公司	4 研制情况	5 平台	6 性能	7 一体化系统的其它配置
AAR-34	红外扫描 8	辛辛那提电子公司 9	50年代末研制 目前收进低温冷却器、处理器 10	F106 EF-111	后视 11	和ALR-62 RWR接口 12
AAR-44	红外扫描 8	辛辛那提公司 9	现役 13	C-130 CH-53	下半球(防地空导弹)W=20.4kg 14	还应用CIDS(MC-130H特种作战飞机综合防御系统), C/DS还包括ALR-69(V) TRWR, APR-46全向接收机, ALE-40以及电子战处理器 15
AAR-Fx	8 红外扫描	辛辛那提公司 9	正在研制 16		W<20kg φ10cm, L50cm双探头系统 17	它采用AAR-34/44的成熟技术 18
SAWS 19 (静默攻击告警系统)	红外扫描 8	洛雷尔通用电气德州仪器 20	各研制一个样制 21	在C-141上一起试验 22		从这三家公司的系统候选出ISAS(综合态势告警器) 23

1. Model. 2. System. 3. Company. 4. Development. 5. Platform. 6. Capabilities. 7. Other combined equipment. 8. Infrared sweep. 9. Cincinnati Electronics. 10. Developed in the 50's. Now with low temperature cooler and processor. 11. Backward looking. 12. Connected to ALR-62 RWR. 13. Currently in service. 14. Lower hemisphere (anti - SAM) W=20.4kg. 15. Also uses CIDS (MC-130H special operational aircraft comprehensive defense system), C/DS also includes ALR-69(V) TRWR, APR-46 omnidirectional receiver, ALE-40 and ECM processor. 16. Under development. 17. W<20kg, diameter 10cm, length 50 cm, dual detector system. 18. Uses AAR-34/44's technology. 19. SAWS (Silent attack warning system). 20. Lowell, GE, Texas Instruments. 21. One prototype/company. 22. Tested on C-141. 23. Select an integrated state alarm system from among these three.

型号 1	体制 2	公司 3	研制情况 4	平台 5	性能 6	一体化的其它配置 7
AAS-43	红外凝视 8	通用电气 9	在试验中 10	原拟装备在A-12上 11	铟化锌128×128传感器 12	它和F-22的IENEWS中的导弹告警器类似 13
蝇眼 14	红外凝视 8	洛克韦尔 15	试验 10	在P-3飞机上试飞 16		作为早期发射告警 17
QQR-47	紫外凝视 8	洛雷尔 18	已完成演示试验 19	直升机运输机AV-8B(计划) 20	采用四个紫外探头，属非冷却型。可扩展至全方位 21	计划和ALQ-199配套(提供拦截时间)。首先AAR-47无源探测，然后由ALQ-199确定TTC并可自动启动干扰物22
DDM-2000	红外凝视 8	法国SAT公司 23	刚在生产 24	幻影—2000CD(特装备) 25	双探头，全方位 26	和DDM-Prime性能相同，结构不同 27
DDM-Prime	红外凝视 8	法国SAT公司 23	研制中 16	"狂风"飞机 28	双探头，全方位，中红外，G-A 1-7km A-A 10-15km t_g = <2°可40跟踪个目标 29	Srecrta一体化自卫系统的一部分，Specra还包括一部正由Thomson-CSF研制中的雷达型MAW 30

1 - 7. Same as previous table. 8. IR fixed vision. 9. GE. 10. Testing. 11. Planned for A-12. 12. Indium zinc compound 128 X 128 sensor. 13. Similar to F-22's missile warning device in INENEWS. 14. Fly eye. 15. Rockwell. 16. Testing on P-3. 17. Early launch warning. 18. Lowell. 19. Demonstration testing complete. 20. Transport AV-8B (planned). 21. Four UV probes, non-cooled. Can be expanded to omnidirectional. 22. Planned to be used with ALQ-199 (provide intercept time). First passive detection by AAR-47, then TTC determination by ALQ-199 and automatically begins jamming. 23. French SAT. 24. Production begun. 25. Phantom-2000CD. 26. Dual probe, omnidirectinal. 27. Capabilities similar to DDM-prime, but structurally different. 28. Tornado. 29. Dual probe, omnidirectional, G-A - 1-7km, A-A - 10-15 km, <2°, can track 40 targets. 30. Part of Scecrta integrated self defense system, also has a radar MAW under development by Thompson.

4.2. Laser warning devices

Laser warning devices are used to detect incoming missiles or aircraft. They are activated by the detection of laser beam radiation. We can see from the Gulf War that the Multinational Forces were bombing ground targets, many of the bombs were laser guided bombs ""Jewel Road"-2 and 3 (GBU-12, GBU-16, GBU-10, and GBU-24) or air-to-surface laser semi-active guided missiles (AGM-65C.E, AS-30, Shiprer, and Hellfire). When using these laser guided weapons, it is necessary to direct a laser beam on the target. Therefore, when the enemy uses a laser guided weapon to attack ground targets, it is necessarily possible to detect the laser beam in the vicinity of the protected target. Therefore, a laser warning device can detect an imminent attack by a laser guided missile. The status of research into laser warning devices in foreign countries is given in the following table.

国别1	名称 2	研制单位 3	特点 4	装备 5
6 英	453型激光报警接收机 7	弗兰蒂公司 8	探测波长0.3～11μm，方位角36°，高低角180°，区域分辨率90或45° 9	旋转翼，固定翼飞机 10
	专用激光报警接收机 11	普莱赛航空电子技术公司 12	探测地基和机载红宝石，钕玻璃激光波长，探测距离约10km。方位角360°高低角45°～10° 13	装甲车 14
	激光和红外探照灯控测器 15	普莱赛雷达公司 16	可接收直接照射激光束，也可用散射探测器接收散射的激光。用于坦克的作用距离大于20km 17	飞机、坦克 18
国	1220激光告警系列 19	Marconi公司 20	多探头使用，可提供360°方位和55°俯仰（－15°～40°）额定角分为率为±22.5°探测波段0.35～1.1μm，可扩展到1～2μm，8～11μm可识别红宝石、GaAs、Nd.YAG等激光 21	

1. Country. 2. Nomenclature. 3. Developer. 4. Characteristics. 5. Platform. 6. England. 7. 433 laser warning receiver. 8. Fuolandi (phonetic) corporation. 9. Detects wavelength 0.3-11μm, azimuth angle 36°, elevation angle 180°, sector discrimination 90° or 45°. 10. Rotary or fixed wing aircraft. 11. Special use laser warning receiver. 12. Pulaisai (phonetic) Aviation Electronics. 13. Detect land-based and airborne ruby and neodymium glass laser wave lengths, detects ranges up to 10km, azimuth angle 360°, elevation angle 40°-10°. 14. Armored vehicles. 15. Laser and infrared searchlight detector. 16. Pulaisai (phonetic) Radar Co. 17. Can receive directly radiated laser beams and can use diffusion detectors to receive diffused laser. On tanks can be used up to 20km. 18. Aircraft and tanks. 19. 1220 Laser warning series. 20 Marconi Co. 21. Multiple probe use, can provide 360° azimuth and 55° elevation (-15°-40°). Detection wave band 0.35-1.1μm. Can be expanded to 1-2μm, 8-11μm. Can recognize ruby, GaAs, Nd:YAG lasers.

1	2	3	4	5
6 西	Alberich 激光报警系统 7	Kurt Eich Weber khein metall Nico Pyrotechnik 8	激光传感器高100mm，截面130mm，可探测的激光波长为0.66～1.1μm方向探测精度在3°以内。与雷达报警接收机组合 9	装甲车 10
	LAWA 激光报警系统 11	埃尔特罗公司 12	探测范围：俯仰+60°～-20°；方位360°；角分辨率0.5° 13	直升机、装甲车 14
德	COLDS 通用光电激光探测系统 15	MBB公司 16	探测红宝石、Nd:YAG激光测距仪，目标指示器、Co_2激光测距仪的波长。360°方位，±45°俯仰、角分为辨3°或1.5° 17	直升机、坦克、舰船 18

1. Country. 2. Nomenclature. 3. Developer. 4. Characteristics. 5. Platform. 6. West Germany. 7. Alberich laser warning system. 8. Kurt Eich Weber khein metall nico Pyrotechnik. 9. Laser sensor is 100mm high, cross section of 130mm, detectable laser wavelength is 0.66 - 1.1μm, azimuth detection precision within 3°. Used in conjunction with radar warning receiver. 10. Armored vehicles. 11. LAWA laser warning system. 12. Aiertemeng (phonetic) Co. 13. Detection range: Elevation +60°- -20°, azimuth 360°, angle resolution 0.5°. 14. Helicopters and armored vehicles. 15. COLDS universal electro-optical laser detection system. MBB Co. 17. Detects wavelengths of ruby and Nd:YAG laser rangers, target indicators, and Co_2 laser rangers. 360° azimuth, ±45° elevation, angular resolution is 3° or 1.5°. 18. Helicopters, tanks, and boats.

1	2	3	4	5
6 美国	AN/AVR-2 激光报警器 7	珀金-埃尔默公司 8	能探测、识别、测定激光源位置与AN/APR-39雷达接收组合，具有视频显示音响报警和机内测试功能。 9	直升机、坦克 10
	轻型激光报警系统 11	休斯公司 12	传感器方位角190°，仰角110°，提供激光威胁的方向，脉冲速率，宽度和强度 13	战术飞机、装甲车、舰船 14
	高精度激光报警器 15	AIL系统公司 LMO光电系统公司 16	探测角精度方位1mrad，俯仰1.5mrad，波长0.4～1.1μm脉宽10～200ns，灵敏度优于1mw/cm²，可同时定位和显示三个威胁 17	
法国 18	DAL激光告警器 19	Thomson公司的SAT 20	探测波长0.65～1.06μm，低虚警概率，体积4000cm³ 21	

1. Country. 2. Nomenclature. 3. Developer. 4. Characteristics. 5. Platform. 6. United States. 7. AN/AVR-2 laser warning device. 8. Pojin-Ai'ermo (phonetic) Co. 9. Can detect, recognize and determine position of laser source. Used in conjunction with AN/APR-39 radar receiver. Has visible light and sound warning and internal testing capability. 10. Helicopters and tanks. 11. Light laser warning system. 12. Houghes Co. 13. Sensor azimuth angle 190°, elevation angle 110°. Wave length 0.4-1.1μm, pulse width 10-200ns. Provides direction, wave length, pulse rate and pulse width and strength of laser threat. 14. Fighters, armored vehicles and ships. 15. High precision laser warning device. 16. AIL system Corporation, LMO Electro-optical Systems Corporation. Detection azimuth angle precision 1 mrad, elevation angle 1.5 mrad. Wave lengths 0.4 - 1.1μm, pulse width 10-200ms. Sensitivity greater than 1mw/cm^2. Can locate and display three threats at one time. 18. France. 19. DAL laser warning device. 20. Thompson Corporation's SAT. 21. Detection wavelength 0.65-1.06μm, low false alarm rate, size 4000 cm2.

5. New infrared decoys

After the Gulf War, the United States military believes that "RF threats are almost under control, but infrared threats have

gradually become even harder to deal with. Certain infrared homing missiles have been developed to a degree where flares cannot draw them off. They use an extremely complex technology to discriminate between the aircraft and the flares, so it is necessary to develop new infrared decoys." The United States Air Force has drafted a new development plan for this, the research projects and development contracts of this plan are listed in the following table.

Item	Developer	Project and contents
1.	Thiocol	Mobile decoy flare contract, completed February, 1993
2.	Lockheed Sanders	Brite/Dim air flare contract, completed February, 1993
3.	Metal Surface Co.	Active metal lure corporation, using crushed metal to form oxidation in air and to radiate infrared. The result is the formation in air of tremendous heat source interference
4.	Rockwell Flare systems	Air flare contract, completed Feb, 1992.
5.	Telake (phonetic)	Infrared imaging decoy. Testing and validation completed. Can be launched by A LE-40 launcher.
6.	Telake	Two part decoy
7.	IMVECE	Infrared imaging decoy
8.	Lowell	LORALEL decoy plan, decoy has automatic pilot capability. Combines flare, RF and infrared countermeasures capability. Can control characteristics of separation. Can be launched by ALE-40 launcher.

The British have developed an explosive type infrared lure, the "shield", which has seven infrared decoy charges inside the shell with electronic timed fuses, and can be exploded in a set time sequence and burn within a certain position in the air forming a 2-14μm infrared radiation decoy cloud.

The French have developed the "Dagai" (phonetic) which is a flung type infrared decoy. It uses the gasses of combustion of

explosives to cast a large amount of infrared decoy smoke and sparks into the air, burning to form an infrared decoy cloud.

These two long wave infrared decoys developed by the British and French take less than one second from ignition to the formation of an infrared decoy. They have high radiation energy, between 3 and 5μm it can reach 2000Watts/Sr, and can form jamming in the 8-14μm band, forming a large area decoy cloud, which can be as large as 300m^2. However, duration is fairly short, 2.5 seconds, so a number of rounds must be fired one after the other.

6. Suppression type infrared countermeasure equipment

One of the major methods of countering precision guided weapons is currently the development of suppression type electro-optical countermeasure equipment. The United States, Soviet Union, Germany and France have already developed a group of strong laser weapons which blind the operator and blind the sensors. They are suppressive type electro-optical countermeasure equipment. The basic status of this equipment is shown in the following table.

序号1	项目 2	国别3	公司 4	性能 5	备注6
1	"虹鱼"车载激光武器系统 7	美 8	马丁、马丽埃塔公司,通用电气公司 9	致盲人员和光电传感器。可以使瞄准具视场内的敌方车辆和传感器中3/4永久性或暂时性致盲 10	装备部队 11
2	"花冠王子"机载激光武器 12	美 8	西屋电气公司研制 13	将"虹鱼"发展为机载 14	
3	直升机载激光致盲系统 15	美 8	陆军 16	在"虹鱼"和"小兰鸟"基础上发展的轻型机载激光武器对抗红外引导的防空导弹 17	
4	机载先进光学干扰吊舱 18	美 8	空军、海军 19	用Nd:YAG激光器,致盲地面射手眼睛,7.5万美元一台 20	完成装置研制 21
5	坦克车载激光武器 22	德 23	MBB	用Co_2气动激光,致盲传感器的距离在20km以上,5km可破坏导弹壳体 24	系统试验 25
6	激光眩目瞄准器 26	英 27	皇家信号和雷达研究所 28	使用Nd:YAG倍频激光器在5km内可使驾驶员眼睛致盲 29	部队使用 30
7	便携式激光眩目器 31	美 8	联合信号公司 32	金绿宝石激光器,重9kg,致盲人眼睛和光电传感器。33	已通过野外试验34
8	激光武器系统 35	法 36	Tlnilaser公司和Laserdot公司 37	用Co_2气动激光,能摧毁几公里内的光学系统,预计1995年完成试验任务。38	

1. Number. 2. Project. 3. Country. 4. Company. 5. Capabilities. 6. Notes. 7. "Hongyu" (phonetic) vehicle carried laser weapons system. 8. United States. 9. Martin Marietta, General Electric. 10. Blinds personnel and electro-optical sensors. Can permanently or temporarily blind 3/4 of the enemy vehicles and sensors within field of view of sights. 11. In hands of units. 12. "Crown Prince" airborne laser weapon. 13. Westinghouse Electric. 14. Airborne version of "Hongyu". 15. Helicopter laser blinding system. 16. Army. 17. Light airborne laser weapon developed on basis of "Hongyu" and "Bluebird" to counter infrared guided air defense missiles. 18. Airborne advanced optical jamming pod. 19.

Air Force, Navy. 20. Uses Nd:YAG laser to blind ground gunners. Costs 75,000 Dollars each. 21. Equipment testing completed. 22. Tank laser weapon. 23. Germany. 24. Uses Co_2 laser to blind sensors at more than 20km. At 5 km it can damage missile casing. 25. System testing. 26. Laser glare sighting device. 27. England. 28. Royal Signals and Radar Institute. 29. Uses Nd:YAG frequency multiplier laser which can blind drivers within 5km. 30. In use in units. 31. Hand carried Laser glare device. 32. United Signals. 33. Metallic emerald laser, weighs 9kg, blinds personnel and electro-optical sensors. 34. Passed field tests. 35. Laser weapon system. 36. France. 37. Tinilaser and Laseriot Cos. 38. Uses Co_2 gas laser, and can destroy optical systems within several kilometers. Estimated that testing will be completed in 1995.

2-18GHz BIPOLARIZED HORN ANTENNAS USED IN ELECTRONIC WARFARE

BY: Teng Xiuwen
(Ministry of Electronics, Institute 29)

I. ABSTRACT

The 2-18GHz bipolarized horn antenna introduced in this article is a new wideband antenna. It has excellent electrical properties within the 2-18GHz band. This article introduces the design methods for this type of antenna and its operational principles. These include the four spine wave guide design method, the horn spread spine design, and the coaxial-spine wave guide converter design. At the same time, this article will also introduce spread spectrum technology, higher mode suppression technology, and finally this article will introduce the antenna properties. This article provides design diagrams and measurements charts.

KEY WORDS: Wide band, bipolarized, four spine horn

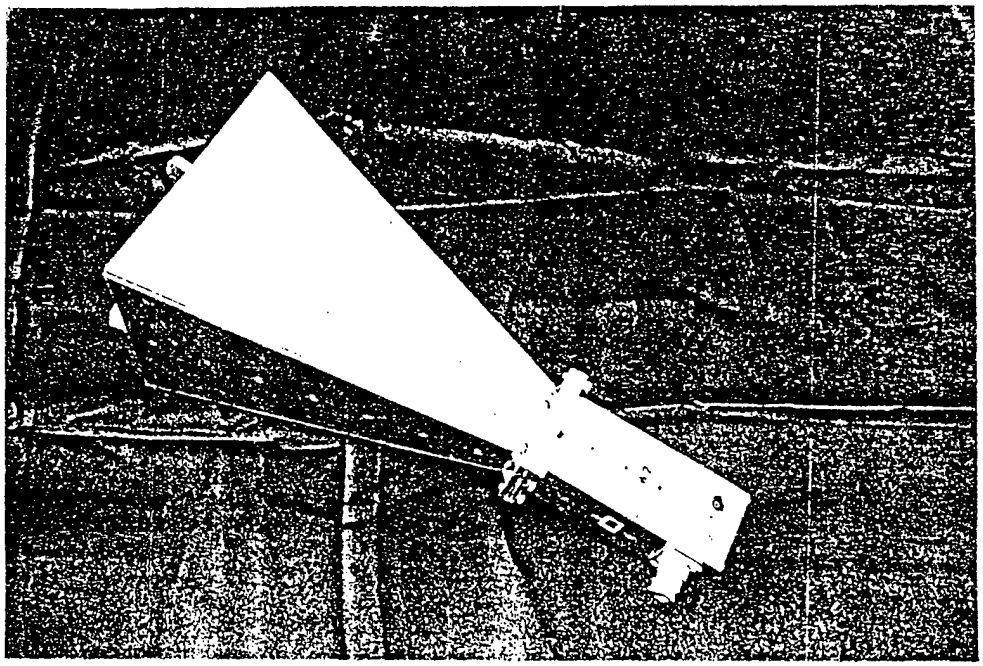
II. Forward

Much of electronic warfare equipment is wideband. For example, the omnidirectional warning equipment operates on the waveband of 2-18GHz, using a plane spiral antenna with a diaphragm. This antenna has an extremely wide frequency band and most of the ground detection equipment uses a horn antenna. The horn antenna has high feed and high size efficiency. However the operating frequencies are generally all fairly narrow, requiring a number of antennas to cover the 2-18GHz waveband, inconvenient for field use.

In order to solve this problem, we began development of a 2-18GHz bipolarized horn antenna. This article will primarily introduce the result of this development.

III. Make-up and operational principles of the antenna

Fig. 1 Wide band four spine horn antenna



A picture of the antenna is shown in Figure 1. This antenna is primarily composed of four spine wave guides, a horn, and a coaxial waveguide converter. The antenna has two input terminals. Within the range of 2-18GHz it has excellent radiation properties and fairly high radiation efficiency. It is especially suited to vehicle carried or shipborne electronic surveillance systems, ground detection systems and laboratory detection systems. Its primary capability indexes are listed in Table 1.

Table 1

1 工作频带	2～18GHz
2 驻　　波	3.5 nom
3 增　　益	>6dB
4 端口数	2
5 隔　　离	20dB(2～12GHz) 15dB(12～18GHz)
6 功率处理能力	1W
7 尺　　寸	140×140×345mm
8 重　　量	1.3Kg

1. Operating frequencies. 2. Standing-wave. 3. Gain. 4. Number of ports. 5. Span. 6. Power handling ability. 7. Dimensions. 8. Weight.

IV. Four spine waveguide parameter selection

The four spine waveguide can be viewed as being composed of two **b/a=1** dual spine waveguides, so we can use the spine waveguide design curve.

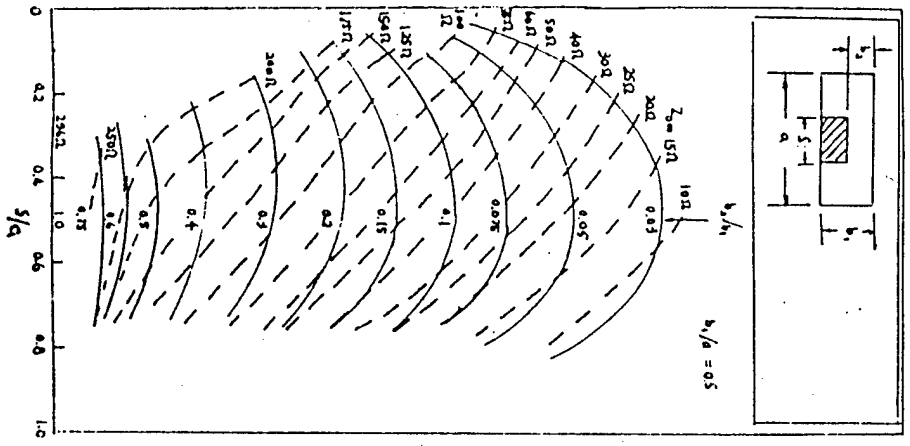
b/a=1 dual spine waveguides can be vied as being composed of two **b/a=0.5** single spine waveguides. Let the dual spine waveguide characteristic impedance be 60Ω, then the characteristic impedance of the single spine waveguide would be 30Ω. From the curve in Figure 2 we can find:

$b_2/b_1=0.03$ $s/a=0.15$

and $b=2b_1$ $d=2d_2$

Therefore, d/b=0.06
s/a=0.15

Fig. 2 Single spine waveguide characteristic impedance



Based on these parameters we can obtain the TE_{10} mode cut-off wavelength of $\lambda_{c10}/a=4.75$, letting the frequency low end cut-off frequency be 1900MHz, the cut-off wavelength is 157.9mm, thus obtaining **a=33.24mm.** We took it to be **a-34mm.** Because the four spine waveguide is square, **b=34mm.**

Because the excitation point was selected at the middle of the waveguide, and by adding a straight wave guide to filter our excited TE_{20}, the dual spine waveguide useable bandwidth should be the ratio of the TE_{10} mode to the TE_{30} mode.

The cut-off wavelength of the TE_{30} mode is $\lambda_{c30}/a=0.775$, so we can calculate $f_{c30}=11.385GHz$. The calculation results indicate that this data only works around 12GHz. To work at 18GHz, it would be necessary to use spread spectrum technology and compensation technology.

It should also be pointed out that this data corresponds to a flat-topped spine, and the actual spines are pointed in order to ensure that there is a mounting gap between the four spines, so the coupling area between the spines is enlarged. Practice has shown that this structure is beneficial to higher order suppression and high frequency band spread spectrum.

V. Design of spines in the expanded portion of the horn

The spines in the horn portion are gradually widened, with the ends bend at the side wall of the horn in order to ensure the broadcast of t^{10} mode. The width of the horn at **H** must be greater than half the wavelength of the lowest operating frequency. In this manner, at the highest operating frequency, it will be several wavelengths. This means that at the mouth there were be a fairly great phase differential. In order to ensure a fairly small phase differential at the mouth, either the horn must be especially long or a lens used to calibrate. However, these are limitations to both these methods. We used a specially designed spine and appropriate compensation measures to do a fairly good job in solving this problem.

The experimentally determined the spine curve is divided into three section. One section is the straight section with a small angle of expansion. The second section is the curved section which follows the equation

$$y=10^{0.00873x+0.78765}+0.3x$$

The third section is the terminal section. It curves at a large angle and terminates at the mouth of the horn.

In the equation, the **x** coordinate is the vertical distance along the center of the antenna to the surface of the spine.

0.03x is the added linear change, serving as spread spectrum compensation. It helps improve low frequency standing-wave and high frequency band higher order suppression.

VI. Wideband coaxial - spine waveguide converter design

Coaxial - spine waveguide converter design is similar to coaxial ordinary waveguide converter design in most aspects. The difference is in impedance. In these two designs, the coaxial line outer conductors are all connected to the sides of the waveguides, and the inner conductors all extend to inside the waveguides forming a single pole radiator. Because ordinary waveguides have an impedance far higher than coaxial impedance, the inner conductor must terminate somewhere far away from the wall of the waveguide in

order to prevent a mismatch. In the spine waveguide, however, the impedance is the same as the coaxial impedance, so the coaxial inner conductor must connect to the corresponding spine.

The key to wideband coaxial - spine waveguide converter design is the design of the back chamber. The impedance of the short circuit section is generally chosen as four to six times that of the waveguide characteristic impedance.

The four spine waveguide uses two port power feed. At one port is the excitation probe is the equivalent of 1/4 wavelength of the highest operating frequency from the short circuit board. At the other port the excitation probe is at a right angle to the first port probe, with the two probes 1.5mm apart. We discovered through experiments that because the second port probe was closer to the short circuit board than the first port probe, and because of the coupling effect between the spines, it was difficult to adjust the characteristics of the standing-wave, and it was necessary to use compensating measures in order to obtain good results.

VII. Measurements of electrical properties

Some of the results of the tests we conducted on the electrical properties of the 2-18GHz bipolarized horn antenna we designed are shown in Figures 3 through 5. We can see from these figures that beyond certain frequency points the antenna standing wave remained at 3.5. The separation between the two ports between the range of 2-12GHz was greater than 20dB. Between 12-18GHz, it was greater than 15dB. We can see from the radiation chart that within the entire frequency range the radiation characteristics are good.

VIII. Conclusions

This article introduces a bipolarized horn antenna which is a newly developed super wideband antenna. It is small, light, has a bandwidth which is especially suited to vehicle carried or shipborne electronic warfare systems and ground and laboratory surveying equipment. During the development of this antenna a number of compensation measures were used which do a fairly good job in solving the problem of higher order modes, so that the antenna has excellent electrical properties within the frequency range of 2-18GHz.

Fig. 3. Standing wave characteristics curve

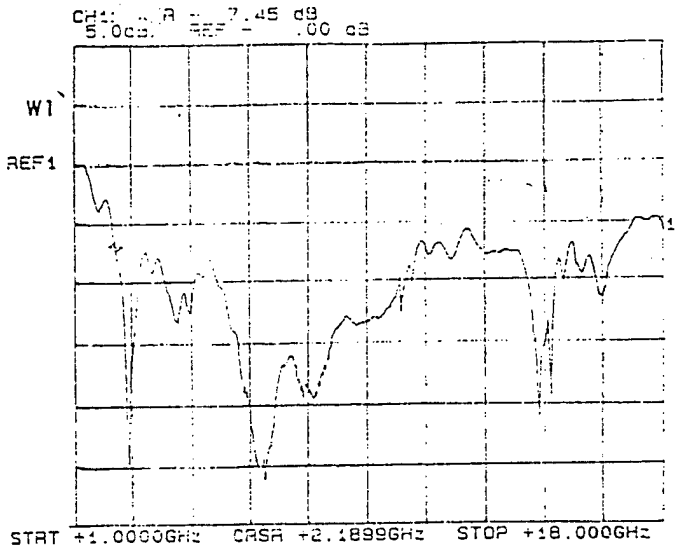


Fig. 4. Separation characteristics curve

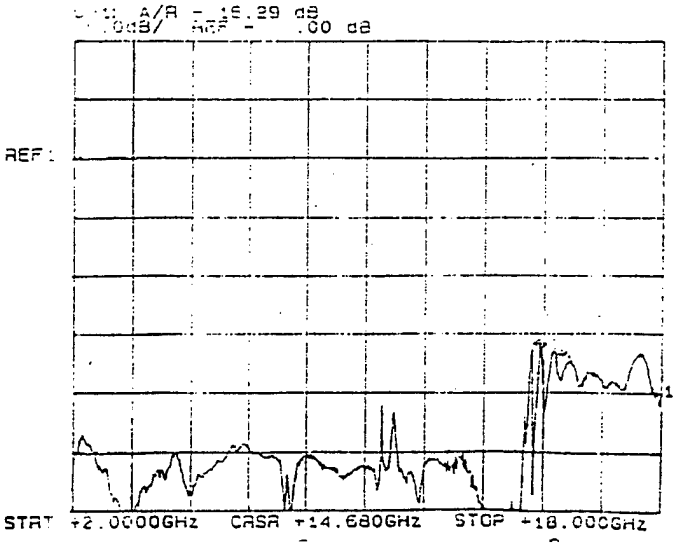


Fig. 5. Radiation charts

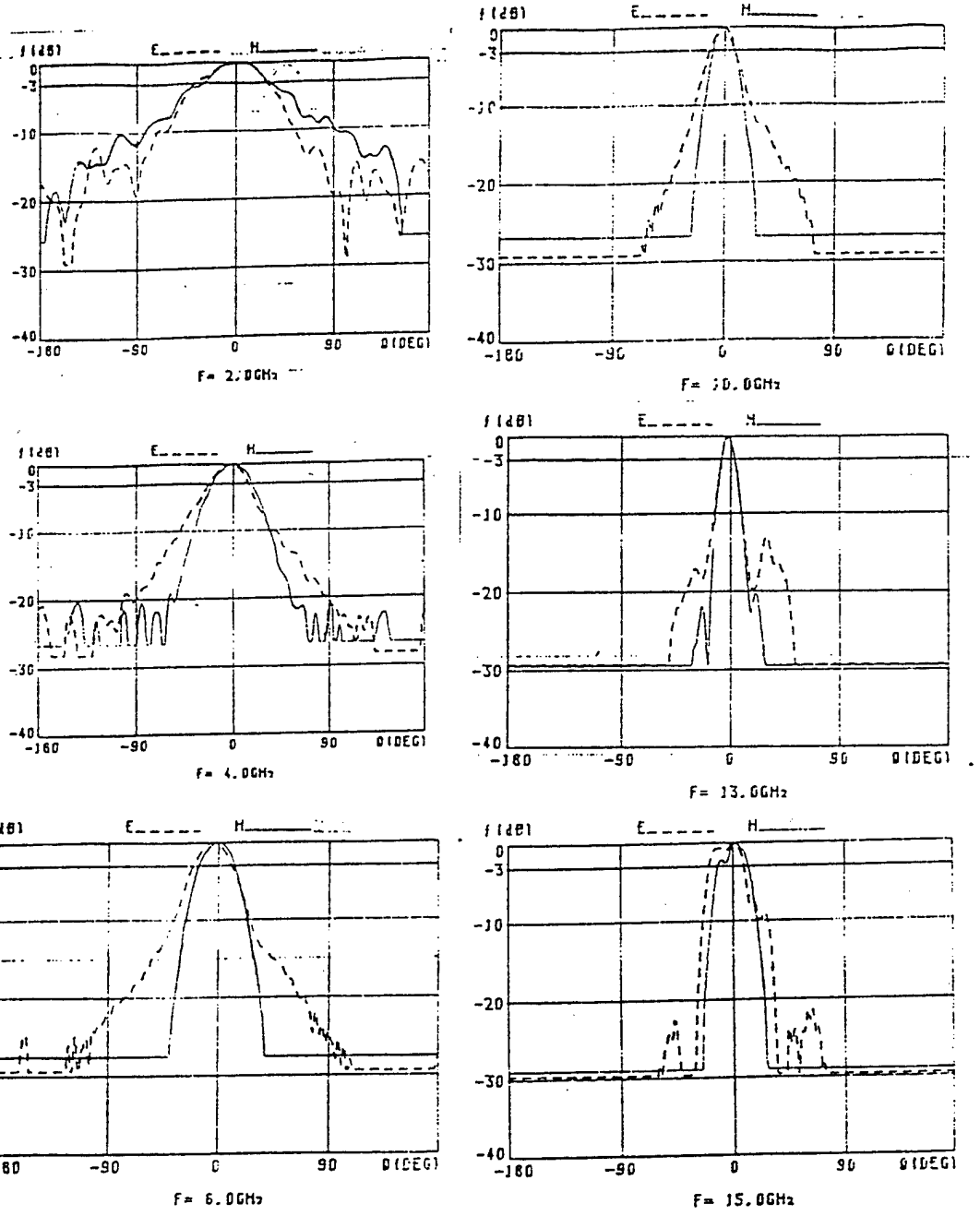


Fig. 5 (continued)